Configuring Frame Relay Services

BayRS Version 12.20
Site Manager Software Version 6.20
BCC Version 4.00

Part No. 117376-C Rev. 00
May 1998

Bay Networks

Bay Networks

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1998 Bay Networks, Inc.

All rights reserved. Printed in the USA. May 1998.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Trademarks

Bay Networks and the Bay Networks logo are trademarks of Bay Networks, Inc.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Bay Networks, Inc. Software License Agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as "Software" in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH BAY NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License Grant. Bay Networks, Inc. ("Bay Networks") grants the end user of the Software ("Licensee") a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Bay Networks Agent software or other Bay Networks software products. Bay Networks Agent software or other Bay Networks software products are licensed for use under the terms of the applicable Bay Networks, Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Bay Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Bay Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Bay Networks' and its licensors' confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Bay Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee's facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Bay Networks warrants each item of Software, as delivered by Bay Networks and properly installed and operated on Bay Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Bay Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Bay Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Bay Networks will replace defective media at no charge if it is returned to Bay Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Bay Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Bay Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Bay Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of

its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL BAY NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF BAY NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF BAY NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO BAY NETWORKS FOR THE SOFTWARE LICENSE.

5. Government Licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of Software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Bay Networks of any such intended examination of the Software and may procure support and assistance from Bay Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Bay Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Bay Networks copyright; those restrictions relating to use and disclosure of Bay Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Bay Networks the Software, user manuals, and all copies. Bay Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and Re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Bay Networks, Inc., 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN BAY NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST BAY NETWORKS UNLESS BAY NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

About This Guide

Before You Begin xv
Conventions xvi
Acronyms xvii
Bay Networks Technical Publications xviii
Bay Networks Customer Service xviii
How to Get Help xix
Bay Networks Educational Services xx

Chapter 1
Starting Frame Relay

Starting Configuration Tools 1-1
Preparing a Configuration File 1-2
Starting Frame Relay 1-2
Configuring PVCs and SVCs 1-6
Configuring a PVC 1-6
Configuring an SVC 1-7
Configuring Adjacent Hosts for an SVC 1-9
Deleting Frame Relay from a Platform 1-9

Chapter 2
Frame Relay Overview

Introduction to Frame Relay 2-2
Permanent Virtual Circuits 2-3
Switched Virtual Circuits 2-3
PVC and SVC Comparison 2-4
Frame Relay Packets 2-5
Management Protocols 2-7

Frame Relay SVC Signaling and LAPF 2-8
LAPF Operational States 2-9
LAPF Timeout and Retransmission Timers 2-10
Timer T200 2-10
Timer T203 2-11
SVC Signaling 2-11
Call Setup 2-12
Message Processing 2-13
Frame Relay Service Records 2-14
Default Service Record 2-14
Multiple Service Records 2-15
Adding and Moving PVCs 2-15
Frame Relay Access Modes 2-15
Group Access Mode 2-15
Direct Access Mode 2-16
Hybrid Access Mode 2-16
Using Hybrid Mode for Transparent Bridging 2-17
Source Routing 2-18
RFC 1490 2-18
Address Resolution for PVCs 2-18
Address Resolution for SVCs 2-19
Traffic Control 2-20
Data Compression 2-21
Data Encryption 2-21
Protocol Prioritization 2-21
Congestion Control 2-22
Traffic Shaping 2-23
Committed Information Rate 2-23
CIR of 0 2-24
Maximum CIR 2-24
CIR Enforcement 2-24
Committed Burst Rate and Excess Burst Rate 2-24
Quality of Service 2-25

Traffic Shaping for SVCs 2-27
Requesting Quality of Service for SVCs 2-27
Refining Quality of Service for SVCs 2-28
Refining Traffic Shaping 2-28
Setting Minimum Acceptable Throughput 2-29
Defining *Incoming* and *Outgoing* *2-29*
Traffic Shaping Considerations 2-29
CIR Configuration Guidelines 2-30
WCP and CIR Enforcement 2-30
Using Traffic Shaping with Data Compression 2-31
Using Traffic Shaping Effectively 2-31
Using Compression Effectively 2-31
Oversubscribing the Interface 2-32
Queue Limits and Data Clipping 2-32
FECN and BECN Notification Bits 2-33
X.213 Priority for SVCs 2-34
Inactivity Timing for SVCs 2-34
Transmit Inactivity Timer and Protocol Priority No-Reset Filter 2-35
Managing Routing Information Protocol (RIP) Over SVCs 2-35
Multiline for PVCs 2-35
Traffic Distribution Between Data Paths 2-36
Random Distribution 2-36
Address-Based Distribution 2-37
Protocol Prioritization and Multiline Incompatibility 2-37
PVC Pass-Through 2-37
Frame Relay Dial Services 2-38
Configuring Synchronous Lines for Frame Relay 2-39
For More Information About Frame Relay 2-39

Chapter 3
Customizing Frame Relay

Using the MIB Object ID 3-1
Selecting a Management Type 3-2
Selecting Address Type and Length 3-4
Selecting a DLCI Address Type 3-4
Selecting Address Length 3-4

Address Type 3-5
Address Length 3-5
Monitoring the Connection 3-6
Polling Interval 3-7
Full Enquiry Interval 3-7
Error Threshold and Monitored Events 3-7
Polling Interval 3-8
Full Enquiry Interval 3-9
Error Threshold 3-9
Monitored Events 3-10
Setting XOFF Control 3-11
Customizing PVCs 3-11
Adding Service Records for PVCs 3-12
Deleting Service Records for PVCs 3-13
Adding PVCs to Service Records 3-14
Deleting PVCs from Service Records 3-16
Moving PVCs from One Service Record to Another 3-17
Enabling Multicast 3-18
Configuring Hybrid Mode for PVCs 3-20
Configuring PVC Pass-Through 3-20
Controlling Congestion for PVCs 3-22
Configuring Congestion Control for an Interface 3-23
Configuring Congestion Control for Individual PVCs 3-25
Using Traffic Shaping With PVCs 3-29
High Queue Limit 3-29
Low Queue LImit 3-30
Committed Burst 3-30
Excess Burst 3-31
CIR (Throughput) 3-31
Enabling Compression for PVCs 3-32
Grouping Service Records for Multiline Mode 3-34
Removing Multiline Services 3-35
Customizing SVCs 3-35
Adding Service Records for SVCs 3-35
Deleting Service Records for SVCs 3-37

Call Screening and Blocking 3-38
SVC Call Block Direction 3-39
SVC Screening 3-39
SVC Screen Usage 3-40
Adding SVC Options to Service Records 3-41
Disabling SVCs 3-42
Disconnecting Active SVCs 3-44
Editing LAPF Parameters for SVCs 3-44
State 3-45
Station Type 3-45
Initiation Mode 3-46
Retransmission Timer 3-46
Idle Timer 3-47
Retransmission Limit 3-47
Information Limit 3-48
Window Size 3-48
Editing Signaling Attributes or Parameters for SVCs 3-50
State 3-50
Maximum SVCs 3-50
Setup Timer 3-51
Disconnect Timer 3-51
Release Timer 3-52
Call Proceeding Timer 3-52
Status Enquiry Timer 3-53
Status Enquiry Retry 3-53
Setting Inactivity Values for SVCs 3-55
Service Record Inactivity Values 3-55
Inactivity Values for an SVC 3-56
Controlling Congestion for SVCs 3-58
Configuring Congestion Control for an Interface 3-59
Configuring Congestion Control for Individual SVC Options 3-61
Using Traffic Shaping with SVCs 3-65
Committed Burst 3-65
Excess Burst 3-66
CIR (Throughput) 3-66

Traffic Shaping Control 3-68
Using Data Compression with SVCs 3-70
Setting X.213 Priorities for SVCs 3-71
Deleting Frame Relay 3-74

Appendix A
Site Manager Parameters

Interface Parameters A-1
Descriptions of Interface Parameters A-4
SVC LAPF Parameters A-11
SVC Signaling Parameters A-17
Parameters for PVCs A-22
Service Name Parameter A-22
Required DLCI Parameter for Each PVC A-24
PVC Service Record Parameters A-26
Optional Algorithm Parameter for Each Multiline Configuration A-32
SVC Service Record Parameters A-34
SVC Service List Parameters A-34
SVC Options Parameters A-40
SVC Options List for Service Parameters A-43

Appendix B
RIP Management for Frame Relay SVCs

Appendix C
Monitoring Frame Relay Using
BCC show Commands

Online Help for show Commands C-1
Commands for Frame Relay C-2
show frame-relay C-4
show frame-relay stats C-16

Index

Figures

Figure 2-1. Frame Relay Network 2-2
Figure 2-2. Frame Relay Header: 2-Byte Format 2-6
Figure 2-3. Frame Relay Header: 3- and 4-Byte Formats 2-6
Figure 2-4. Structure of the DLCMI 2-7
Figure 2-5. Frame Relay Signaling and LAPF Standards 2-8
Figure 2-6. Hybrid Mode Configuration, Non-Fully Meshed Network 2-17
Figure 2-7. Example of a Bridged Network 2-17
Figure 2-8. Big Pipe/Little Pipe Topology 2-20
Figure 2-9. Detecting and Controlling Network Congestion 2-22
Figure 2-10. Traffic Shaping Queues 2-26
Figure 2-11. FECNs and BECNs in Big Pipe/Little Pipe Topology 2-33
Figure 2-12. Multiline Network 2-35
Figure 2-13. PVC Pass-Through 2-38
Figure A-1. Frame Relay Interface List Window (for PVCs) A-2
Figure A-2. Frame Relay Interface List Window (for SVCs) A-3
Figure A-3. FR LAPF Parameters Window A-12
Figure A-4. Frame Relay Signaling Parameters Window A-17
Figure A-5. Frame Relay Service List Window (for PVCs) A-23
Figure A-6. Frame Relay PVC Add Window A-24
Figure A-7. FR PVC List for Service Window A-26
Figure A-8. Services Multiline With Window A-32
Figure A-9. Add Multiline Services Window A-33
Figure A-10. Frame Relay Service List Window (for SVCs) A-35
Figure A-11. Frame Relay SVC Options Add Window A-40

Tables

Table 2-1. PVC and SVC Protocol and Feature Support 2-4
Table 2-2. LAPF Timeout and Retransmission Timers 2-10
Table 2-3. Network Timers 2-12
Table 2-4. Message Processing 2-13
Table 2-5. How Protocols Handle Address Resolution 2-19
Table 2-6. Incoming and Outgoing 2-29
Table 2-7. Inactivity Timer and Inactivity Timer Mode Interaction 2-34
Table 2-8. Synchronous Line Parameters for Frame Relay 2-39
Table B-1. RIP Parameters B-2
Table C-1. Frame Relay Show Commands C-2

About This Guide

If you are responsible for configuring frame relay, you need to read this guide.

If you want to	Go to
Start frame relay on a router with default settings for interface parameters	Chapter 1
Learn about the frame relay protocol, including special aspects of the Bay Networks implementation of frame relay	Chapter 2
Change default settings for frame relay parameters	Chapter 3
Get information about Site Manager parameters (this is the same information that is in Site Manager online Help)	Appendix A

Before You Begin

Before configuring frame relay services guide with a new router, you must complete the following procedures:

- Install the router (see the installation guide that came with your router).
- Connect the router to the network and create a pilot configuration file (see *Quick-Starting Routers*, *Configuring BayStack Remote Access*, or *Connecting ASN Routers to a Network)*.

Make sure that you are running the latest version of Bay Networks Site Manager and router software. If you need to upgrade, see *Upgrading Routers from Version 7–11.xx to Version 12.00*.

Conventions

bold text	Indicates text that you need to enter, command names, and buttons in menu paths. Example: Enter **wfsm &**
	Example: Use the **dinfo** command.
	Example: ATM DXI > Interfaces > **PVCs** identifies the PVCs button in the window that appears when you select the Interfaces option from the ATM DXI menu.
brackets ([ ])	Indicate optional elements. You can choose none, one, or all of the options.
italic text	Indicates variable values in command syntax descriptions, new terms, file and directory names, and book titles.
quotation marks (“ ”)	Indicate the title of a chapter or section within a book.
`screen text`	Indicates data that appears on the screen. Example: `Set Bay Networks Trap Monitor Filters`
separator (>)	Separates menu and option names in instructions and internal pin-to-pin wire connections. Example: Protocols > AppleTalk identifies the AppleTalk option in the Protocols menu.
	Example: Pin 7 > 19 > 20
vertical line (|)	Indicates that you enter only one of the parts of the command. The vertical line separates choices. Do not type the vertical line when entering the command. Example: If the command syntax is
	show at routes | **nets**, you enter either **show at routes** or **show at nets**, but not both.

Acronyms

ANSI	American National Standards Institute
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
B_c	committed burst rate
B_e	excess burst
BECN	backward explicit congestion notification
BofL	Breath of Life (message)
CCITT	International Telegraph and Telephone Consultative Committee (now ITU-T)
C/R	command/response bit
CIR	committed information rate
CRC	cyclic redundancy check
DCE	data communications equipment
DE	discard eligibility
DLCI	data link connection identifier
DLCMI	Data Link Control Management Interface
DTE	data terminal equipment
EA	extended address bit
FECN	forward explicit congestion notification
FRAD	frame relay access devices
FTP	File Transfer Protocol
HSSI	High-Speed Serial Interface
IP	Internet Protocol
IPX	Internet Packet Exchange
ISDN	Integrated Services Digital Network
ITU-T	International Telecommunication Union–Telecommunications (formerly CCITT)
LAN	local area network
LAPF	link access procedure, frame mode
LMI	Local Management Interface
MAC	media access control
MIB	management information base

OSI	Open Systems Interconnection
PRI	Primary Rate Interface
PVC	permanent virtual circuit
QoS	quality of service
SABME	set asynchronous balanced mode extended
SNA	Systems Network Architecture
SVC	switched virtual circuit
TelNet	Telecommunications Network
TFTP	Trivial File Transfer Protocol
UA	unnumbered acknowledgment
URL	uniform resource locator
VC	virtual circuit
WAN	wide area network
WCP	WAN Compression Protocol
WEP	WAN Encryption Protocol
XNS	Xerox Networking System

Bay Networks Technical Publications

You can now print technical manuals and release notes free, directly from the Internet. Go to *support.baynetworks.com/library/tpubs*. Find the Bay Networks products for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Using Adobe Acrobat Reader, you can open the manuals and release notes, search for the sections you need, and print them on most standard printers. You can download Acrobat Reader free from the Adobe Systems Web site, *www.adobe.com*.

Documentation sets and CDs are available through your local Bay Networks sales office or account representative.

Bay Networks Customer Service

You can purchase a support contract from your Bay Networks distributor or authorized reseller, or directly from Bay Networks Services. For information about, or to purchase a Bay Networks service contract, either call your local Bay Networks field sales office or one of the following numbers:

Region	Telephone number	Fax number
United States and Canada	800-2LANWAN; then enter Express Routing Code (ERC) 290, when prompted, to purchase or renew a service contract 978-916-8880 (direct)	978-916-3514
Europe	33-4-92-96-69-66	33-4-92-96-69-96
Asia/Pacific	61-2-9927-8888	61-2-9927-8899
Latin America	561-988-7661	561-988-7550

Information about customer service is also available on the World Wide Web at *support.baynetworks.com*.

How to Get Help

If you purchased a service contract for your Bay Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Bay Networks service program, call one of the following Bay Networks Technical Solutions Centers:

Technical Solutions Center	Telephone number	Fax number
Billerica, MA	800-2LANWAN	978-916-3514
Santa Clara, CA	800-2LANWAN	408-495-1188
Valbonne, France	33-4-92-96-69-68	33-4-92-96-69-98
Sydney, Australia	61-2-9927-8800	61-2-9927-8811
Tokyo, Japan	81-3-5402-0180	81-3-5402-0173

Bay Networks Educational Services

Through Bay Networks Educational Services, you can attend classes and purchase CDs, videos, and computer-based training programs about Bay Networks products. Training programs can take place at your site or at a Bay Networks location. For more information about training programs, call one of the following numbers:

Region	Telephone number
United States and Canada	800-2LANWAN; then enter Express Routing Code (ERC) 282 when prompted 978-916-3460 (direct)
Europe, Middle East, and Africa	33-4-92-96-15-83
Asia/Pacific	61-2-9927-8822
Tokyo and Japan	81-3-5402-7041

Chapter 1
Starting Frame Relay

The quickest way to begin using frame relay on your network is to enable it with default values for all interface parameters and with a default service record that includes at least one permanent virtual circuit (PVC) or switched virtual circuit (SVC). The topics that follow describe this procedure.

Topic	Page
Starting Configuration Tools	1-1
Preparing a Configuration File	1-2
Starting Frame Relay	1-2
Configuring PVCs and SVCs	1-6
Configuring Adjacent Hosts for an SVC	1-9
Deleting Frame Relay from a Platform	1-9

Starting Configuration Tools

Before configuring frame relay services, see the appropriate user guide for instructions on how to start and use the Bay Networks configuration tool of your choice.

Configuration Tool	User Guide
Bay Command Console (BCC)	*Using the Bay Command Console*
Site Manager	*Configuring and Managing Routers with Site Manager*

These guides also describe generally how to create and modify a device configuration.

Preparing a Configuration File

To prepare a configuration file:

1. **Create and save a configuration file that has at least one WAN interface.**
2. **Retrieve the configuration file in local, remote, or dynamic mode.**

For information on these procedures, see the *Quick-Start Routers*.

Starting Frame Relay

You can use either the BCC or Site Manager to start frame relay using default values for all parameters. Frame relay will automatically find out about PVCs from the frame relay switch, and will place the PVCs into the default service.

Using the BCC

To enable frame relay:

1. **Configure a physical interface on an available slot/connector.**

   To configure a physical interface on a slot and connector, navigate to the top-level box prompt and enter:

   <interface_type> **slot** <*slot_number*> **module** <*module_number*> **connector** <*connector_number*>

   <interface_type> is the name of a link- or net-module on the router.

   <slot_number> is the number of the slot on which the link module is located.

   <module_number> is the number of the module on which the slot is located.

   <connector_number> is the number of a connector on the link module.

   After you configure a physical interface, the BCC returns a prompt that specifies your current working location. For example, the following command configures a serial interface on slot 1, connector 2.

```
box# serial slot 1 connector 2
serial/1/2#
```

2. **Configure a frame relay interface on the physical interface.**

   To configure a frame relay interface on a physical interface, navigate to the prompt for the physical interface (for example, box; serial 1/2) and enter:

   frame-relay

   For example:

```
serial1/2# frame-relay
frame-relay/1/2#
```

You have enabled frame relay.

3. **Use frame relay.**

   Frame relay is completely configured with supplied default values. You can use frame relay with the current default settings, or you can customize frame relay to meet the specific needs of your network.

   To determine which frame relay interface attributes that you can configure and what their current values are, enter the **info** command:

```
frame-relay/1/2# info
state enabled
  debug-options none
  trace-options none
  address-length 2
  congestion-timer 1
  address-type q922
  multicast-control disabled
  congestion-control disabled
  congestion-counter 20
  hangup-on-dlcmi-failure disabled
  congestion-method shutdown
  traffic-shaping-timer 128
  high-queue-limit 30
  normal-queue-limit 200
  low-queue-limit 30
```

To determine what other services you can configure under frame relay, enter the **help tree** command and the BCC will display available services. For example:

```
frame-relay/1/2# help tree
The configuration tree below this context is:
  dlcmi
  signalling
  lapf
  default-service
    pvc
    svc-options
    ip
```

```
        rip
        ospf
          neighbor
        arp
        igmp
          relay
      ipx
        rip
        sap
        static-route
        adjacent-host
        static-service
        route-filter
        service-network-filter
        service-name-filter
    service
      pvc
      svc-options
      ip
        rip
        ospf
          neighbor
        arp
        igmp
          relay
      ipx
        rip
        sap
        static-route
        adjacent-host
        static-service
        route-filter
        service-network-filter
        service-name-filter
  service
      pvc
      svc-options
      ip
        rip
        ospf
          neighbor
        arp
        igmp
          relay
      ipx
        rip
        sap
        static-route
        adjacent-host
        static-service
        route-filter
        service-network-filter
        service-name-filter
```

```
ipxwan
  rip
  sap
  static-route
  adjacent-host
  static-service
  route-filter
  service-network-filter
  service-name-filter
backup-circuit
  out-phone-number
  schedule
  caller-resolution
```

You can now configure PVCs and SVCs. You can also specify the protocols you want to run on this interface.

Using Site Manager

To enable frame relay:

1. **Select a link- or net-module connector that requires a WAN circuit.**
2. **Specify frame relay as the WAN protocol by completing the tasks in the following table:**

Site Manager Procedure	
You do this	**System responds**
1. Choose a link- or net-module.	The Protocol window opens.
2. Choose **Frame Relay** and click on **OK.**	The Select Protocols window opens.

You have enabled frame relay. You can now configure PVCs and SVCs. You can also specify the protocols you want to run on this interface.

Protocol prioritization is enabled automatically when you select frame relay. For detailed information on protocol prioritization, see *Configuring Traffic Filters and Protocol Prioritization.* See the appropriate configuration guides for information on configuring the protocols you want to run on this interface.

Configuring PVCs and SVCs

You configure permanent virtual circuits (PVCs) and switched virtual circuits (SVCs) after you enable frame relay.

Configuring a PVC

You can configure PVCs using either the default service record or by adding a service record. Use these instuctions to configure PVCs on the default service record. To configure PVCs on service records that you add, see "Adding PVCs to Service Records" on page 3-14.

Using the BCC

To add a PVC to the default service record:

1. **Navigate to the frame-relay prompt.**

   For example:

   ```
   box; frame-relay/1/2
   ```

2. **Navigate to the default-service prompt.**

   The BCC context changes to the default service record. For example:

   ```
   frame-relay/1/2# default-service
   default-service/1/2#
   ```

3. **Enter the pvc dlci** *<value>* **command.**

   The service provider supplies the data link connection identifier (DLCI), which uniquely identifies this PVC. See **Help** or the DLCI Number parameter in Appendix A for more information.

   For example:

   ```
   default-service/1/2# pvc dlci 16
   pvc/1/2/16#
   ```

You have added a PVC to the default service record. Repeat this procedure to add more PVCs according to the requirements of your network.

Using Site Manager

To configure a PVC:

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Choose **PVCs** > **Add.**	The Frame Relay PVC List for Service window opens.
5. Choose **Add.**	The Frame Relay PVC Add window opens.
6. Enter a value in the **DLCI Number** parameter. See **Help** or the parameter description in Appendix A.	
7. Click on **Done.**	You return to the Frame Relay PVC Add window.
8. Add more PVCs as your network requires. When you are finished, click on **Done**.	You return to the PVC List for Service window.
9. Click on **Done**.	You return to the Frame Relay Service List window.
10. Click on **Done**.	You return to the Frame Relay Circuit Definition window.
11. Click on **Done**.	You return to the main Configuration Manager window.

Configuring an SVC

You can configure SVCs using either the default service record or by adding a service record. Use these instructions to configure SVCs on the default service record. To configure SVCs on service records that you add, see "Adding SVC Options to Service Records" on page 3-41.

Using the BCC

To add an SVC to the default service record:

1. **Navigate to the frame-relay prompt.**

   For example:

   ```
   box; frame-relay/1/2
   ```

2. **Navigate to the default-service prompt.**

   The BCC context changes to the default service record. For example:

   ```
   frame-relay/1/2# default-service
   default-service/1/2#
   ```

3. **Enter the svc-control enable command.**

   This command creates an SVC.

4. **Enter the svc-local-address command.**

You have added an SVC to the default service record. Repeat this procedure to add more SVCs according to the requirements of your network.

Using Site Manager

To configure an SVC:

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Set the **SVC Support** parameter to **Enable**.	The SVC parameters become available.

Site Manager Procedure *(continued)*	
You do this	**System responds**
5. Supply values for the following SVC parameters. Use **Help** or the parameter descriptions in Appendix A. • **SVC Local Party Number** • **SVC Local Party Sub-Address** (optional) • **SVC Local Party Number Plan** • **SVC Local Party Type of Number**	
6. Click on **Apply**.	The SVC button replaces the Multiline button in the Frame Relay Service List window.

Configuring Adjacent Hosts for an SVC

An adjacent host is a device on a locally attached network; it may or may not be a router. You configure a MAC address for each adjacent host that does not implement ARP, or to preempt the ARP process.

If you are configuring IP or IPX for this frame relay service record, see *Configuring IP Services* or *Configuring IPX Services* for instruction on configuring adjacent hosts.

Deleting Frame Relay from a Platform

To delete frame relay from *all* circuits on which it is currently configured:

Site Manager Procedure	
You do this	**System responds**
1. Choose **Configuration Manager** > **Protocols** > **Frame Relay** > **Delete Frame Relay**.	A window prompts: `Do you REALLY want to delete Frame Relay?`
2. Click on **OK**.	The Configuration Manager window opens. Frame relay is no longer operating on the platform.

Chapter 2
Frame Relay Overview

The following sections present an overview of frame relay.

Topic	Page
Introduction to Frame Relay	2-2
Permanent Virtual Circuits	2-3
Switched Virtual Circuits	2-4
PVC and SVC Comparison	2-4
Frame Relay Packets	2-5
Management Protocols	2-7
Frame Relay SVC Signaling and LAPF	2-8
SVC Signaling	2-11
Frame Relay Service Records	2-14
Frame Relay Access Modes	2-15
Source Routing	2-18
RFC 1490	2-18
Address Resolution for PVCs	2-18
Address Resolution for SVCs	2-19
Traffic Control	2-20
Data Compression	2-21
Data Encryption	2-21
Protocol Prioritization	2-21
Congestion Control	2-22
Traffic Shaping	2-23
Traffic Shaping for SVCs	2-27

Topic	Page
Traffic Shaping Considerations	2-29
X.213 Priority for SVCs	2-34
Inactivity Timing for SVCs	2-34
Multiline for PVCs	2-35
PVC Pass-Through	2-37
Frame Relay Dial Services	2-38
Configuring Synchronous Lines for Frame Relay	2-39
For More Information About Frame Relay	2-39

Introduction to Frame Relay

Frame relay is a high-speed, packet-switching WAN protocol that connects geographically dispersed LANs. Frame relay is usually offered by a public network provider; however, private organizations can acquire and manage their own frame relay networks as well.

Frame relay is a connection-oriented protocol, which means that it relies on end-to-end paths between devices connected across the network. It implements these connections using permanent virtual circuits or switched virtual circuits.

Figure 2-1 illustrates a frame relay network.

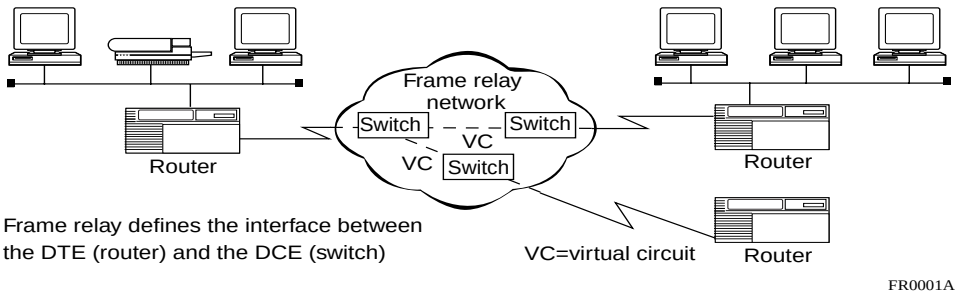

Figure 2-1. Frame Relay Network

Frame relay assumes that networks use transmission lines with low error rates, such as digital transmission media. Consequently, frame relay provides only basic error detection with no error recovery. This minimizes the processing required for each packet, allowing frame relay networks to operate at high speeds with few network delays.

Because frame relay performs only basic error checking, end stations running upper-layer protocols such as Internet Protocol (IP) are responsible for resending packets that did not transmit correctly the first time.

Permanent Virtual Circuits

A *permanent virtual circuit* (PVC) is a dedicated logical path that connects two devices over a network. Once configured, a PVC is always available to the connected devices; a PVC does not require setup before data can travel across the network, nor a disconnect after. Since many PVCs can coexist, devices can share the bandwidth of the transmission line.

Switched Virtual Circuits

A *switched virtual circuit* (SVC) is a logical path that is established on an as-needed basis. That is, an SVC exists only when there is data to transfer. SVCs can connect any two points on a network without the requirement that the provider preconfigure *virtual circuits* (VCs).

SVCs can provide an alternative to a large network infrastructure, potentially resulting in cost savings for networks with infrequent communications between sites. SVCs can also provide an easy and relatively inexpensive solution for disaster recovery. Costs associated with having a redundant PVC are eliminated. In addition, you can prepare an SVC network for disaster recovery by performing incremental backups to a mirror-image database on a remote server.

In addition to cost savings, SVCs provide other benefits. When frame relay networks using global addressing approach a thousand sites, they run out of data link connection identifiers (DLCIs). SVCs enable you to manage connectivity on the basis of use rather than permanent connections. Using SVCs also simplifies network administration because you do not have to preconfigure network topologies and support moves, adds and changes, as with PVCs. This can be a significant benefit in large, highly meshed networks.

SVCs provide true bandwidth-on-demand service that can be customized based on the application in use. For example, a short interactive session might use an SVC with a low or zero committed information rate (CIR) or throughput rate, while a large file transfer of time-critical data might require an SVC at a high CIR value.

PVC and SVC Comparison

Table 2-1 lists the protocols and features that PVCs and SVCs support.

Table 2-1. PVC and SVC Protocol and Feature Support

Protocol/Feature	PVCs Support	SVCs Support
IP, IPX	✔	✔
AppleTalk APPN Bridging DECnet DLSw OSI VINES XNS	✔	
Data compression (WCP)	✔	✔
Data encryption (WEP)	✔	
Protocol prioritization	✔	✔
Dial-on-demand	✔	✔
Dial backup	✔	✔
Congestion control	✔	✔
Traffic shaping	✔	✔
PVC pass-through	✔	
Multiline	✔	

Frame Relay Packets

Figure 2-2 illustrates the structure of a frame relay packet. The packet's header field includes the following:

- *Data link connection identifier (DLCI)*

  The DLCI is the virtual circuit identification number. The frame relay network uses the DLCI to direct basic data flow. You configure the DLCI for PVCs. For SVCs, the frame relay switch assigns the DLCI number on a per call basis.

- *Command/response bit (C/R)*

  ITU-T (formerly CCITT) standards do not use this bit.

- *Forward explicit congestion notification (FECN)* and *backward explicit congestion notification (BECN)*

  The FECN and BECN indicate congestion on the network. For information about how the frame relay software uses these bits, see "Congestion Control," on page 2-22.

- *Discard eligibility (DE)*

  The DE bit allows the router to mark specific frames as low priority (discard eligible) before transmitting them to the frame relay network.

- *Extended address bit (EA)*

  The EA bit signals whether the next byte is part of the address. This bit indicates the last byte of the DLCI.

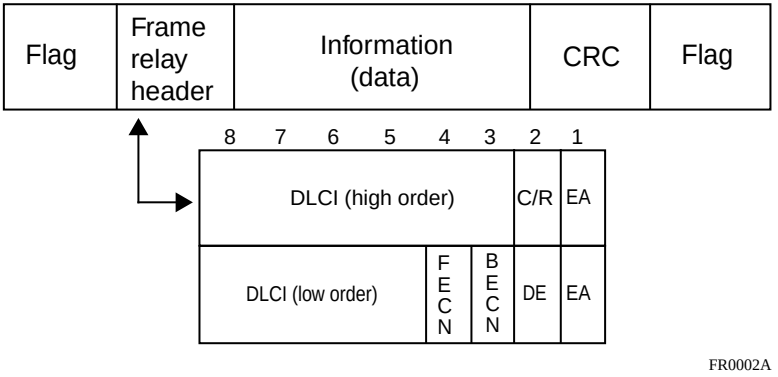

Figure 2-2. Frame Relay Header: 2-Byte Format

Figure 2-2 shows the frame relay header as a 2-byte structure. Frame relay can also format the header using 3 or 4 bytes, as shown in Figure 2-3. Note, however, that you must configure the frame relay interface on the router to use the same header length as the switched network to which it is connected.

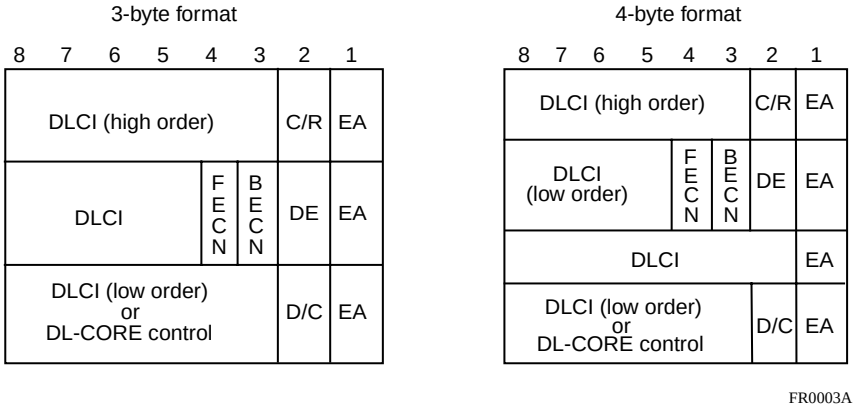

Figure 2-3. Frame Relay Header: 3- and 4-Byte Formats

Management Protocols

Frame relay is an access protocol that runs between a router or data terminal equipment (DTE) and a switch or data communications equipment (DCE). The router and the switch use the Data Link Control Management Interface (DLCMI) to exchange information about the interface and the status of each virtual circuit (Figure 2-4).

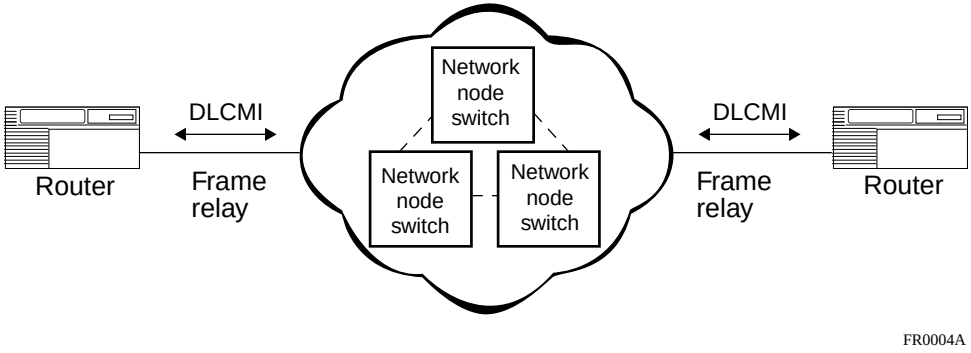

Figure 2-4. Structure of the DLCMI

DLCMI supports three standard data link management specifications: LMI, ANSI T1.617 Annex D, and CCITT (now ITU-T) Q.933 Annex A.

- The networking industry first developed the *Local Management Interface (LMI)* specification. The LMI approach is asymmetric; the router sends a status-inquiry message to the network, signaling that the router's connection to the network is functioning. The network replies with a status response.
- ANSI modified the LMI specification and incorporated it as Annex D to ANSI standard T1.617. The ANSI method is generally similar to the LMI approach.
- The CCITT (now ITU-T) modified the ANSI standard and adopted it as Annex A to Q.933. The CCITT Annex A specification is similar to Annex D, but it uses an international numbering scheme.

Be sure to configure the frame relay interface on the router to use the same management protocol as the switched network to which it is connected. For information about configuring frame relay, see Chapter 3, “Customizing Frame Relay.”

Frame Relay SVC Signaling and LAPF

Figure 2-5 shows the layers of protocol standards for frame relay signaling:

- The LAPF Core layer defines basic frame relay protocol for both PVCs and SVCs and supports the reliable transfer of multiple numbered frames over SVCs.
- The DLCMI layer defines link management protocol for PVCs.
- The LAPF and Q.933 layers define link management protocol for SVCs.

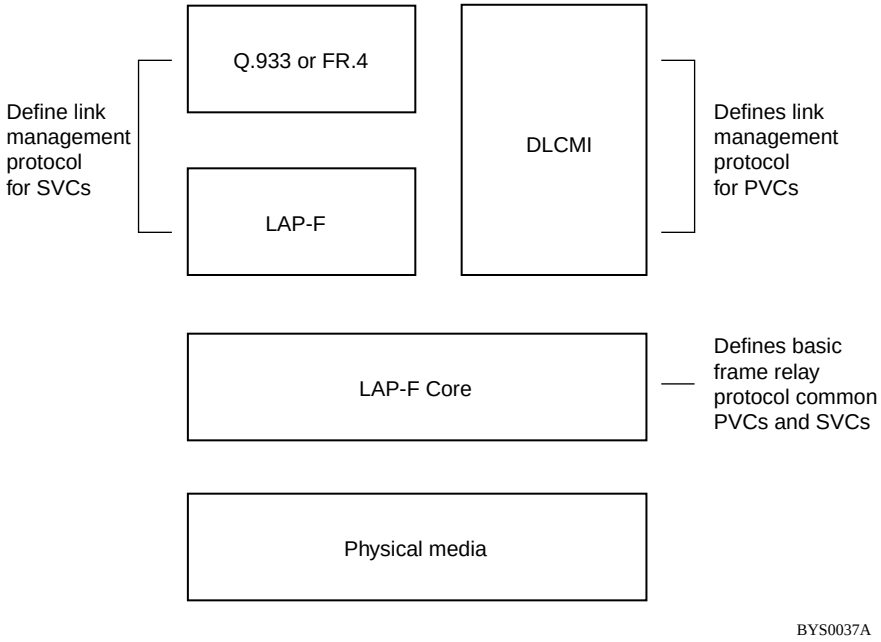

Figure 2-5. Frame Relay Signaling and LAPF Standards

The link access procedure, frame mode (LAPF) layer defines five unnumbered control frames and three numbered supervisory frames on the communications link.

LAPF defines the following categories of management frames to support reliable transfer of multiple numbered frames over SVCs:

- *Unnumbered control* - Provides connection and disconnection services and includes set asynchronous balanced mode extended (SABME), disconnect (DISC), frame reject (FRMR), disconnected mode (DM), and unnumbered acknowledgment (UA) frames.
- *Numbered supervisory* - Provides flow control and retransmission information and includes receiver not ready (RNR), receiver reader (RR), and reject (REJ) frames.
- *Numbered information (I)* - A numbered command/response which passes data across the link using a sliding window protocol. The frames are numbered sequentially and carry an acknowledgment of the highest numbered frame received by the sending peer. The maximum number of frames outstanding is configurable. These frames can only be sent after setup of multiple frame communications on the link. A flag within the frame differentiates a command from its response.
- *Exchange identification (XID)* - An unnumbered command/response used to allow peers to exchange identification information.

LAPF Operational States

LAPF has three main operational states:

- *TEI-assigned* - This is the base interface state. When the LAPF circuit is first established, this is its state. No timers are running and only unnumbered frames are supported across the link.
- *Active* - This state indicates that multiple frame support is up and running on the interface. Numbered information frames can travel across the link.
- *Timer recovery* - This state indicates that a timer has expired and the peer is attempting to recover either through retransmission (T200 timeout) or by initiating an idle time handshake (T203 timeout).

Once multiple frame support is operating on the channel, numbered information frames are exchanged to transfer data and acknowledge earlier transfers.

LAPF Timeout and Retransmission Timers

Table 2-2 lists the timers and retransmission limits defined in the LAPF protocol for timeouts and retransmissions.

Table 2-2. LAPF Timeout and Retransmission Timers

Site Manager Parameter	Description
T200	This general purpose retransmission timeout is used during initiation of LAPF multiple frame support and for timeout of numbered information frames.
T203	This timeout detects excessive idle time on the line and initiates a frame handshake to check if the connection is still up.
N200	This maximum retransmission count, when reached, causes the software to take action. The action take by the router software depends on the type of message timed out and the state of the service.

Timer T200

Timer T200 detects transmission timeouts. When a timeout occurs, the peer enters the timer recovery state and retransmits the frame, up to a maximum of N200 times. If this limit is reached, the system performs the following operations:

- Terminates multiple frame operation
- Discards all outstanding information frames
- Transitions the peer to the TEI-assigned state
- Initiates multiple frame setup

If the remote peer receives a frame that contains an error, it sends an REJ message to specify which frame was in error. In response, the local peer retransmits information frames, beginning with the bad frame.

If the remote peer encounters an error which retransmission cannot remedy, it sends an FRMR response to the local peer and transitions to the TEI-assigned state. The local peer discards all outstanding information frames, transitions to the TEI-assigned state, and initiates multiple frame setup.

The supervisory frames, RNR and RR, support flow control on the channel. If the receiver is not ready to receive data, it sends an RNR message to tell the sender to wait. When it is ready to receive data, it sends an RR message. Flow control in one direction is independent of the other direction.

Timer T203

Timer T203 is used to detect a lost connection. When either end of the link is not waiting for any data, it starts timer T203. If it sends or receives no frames before this timer expires, the peer transitions to the timer recovery state, sends either an RR or RNR message to the remote peer, and starts timer T200. If timer T200 expires, the connection is assumed lost, and the peer transitions to the TEI-assigned state.

To terminate multiple frame support on the circuit, one peer sends a DISC message to the other. The receiving peer responds with a UA message, and disconnects the circuit.

SVC Signaling

The following sections describe the signaling between a DTE and the frame relay network in which various types of messages are exchanged.

Table 2-3 contains a list of timers used in the signaling exchanges that occur. You can use Site Manager to configure these timers to your specific requirements.

Call Setup

A frame relay SVC is established using the frame relay signaling protocol between the subscriber (DTE) and the network. This protocol is described in the sections that follow. The timers used in this process are summarized in Table 2-3 (column 1, *Timer*, contains the Site Manager parameter name).

Table 2-3. Network Timers

Timer	Default Time-Out	State of Call	Cause for Start	Normal Stop	At First Expiration	At Second Expiration
T303	4 sec	Call present	Outgoing setup message	Incoming connect, call proceeding, or release message	Retransmit setup message; restart timer T303	Clear call
T305	30 sec	Disconnect indication	Outgoing disconnect message	Incoming disconnect or release message	Network sends release message	Timer not restarted
T308	4 sec	Release request	Outgoing release message	Incoming release or release complete message	Retransmit release message; restart timer T308	Call cleared; timer not restarted
T310	10 sec	Incoming call proceeding	Incoming call proceeding message	Incoming connect or disconnect message	Call cleared	Timer not restarted
T322	4 sec	Any state	Outgoing status inquiry message	Incoming status, disconnect, release, or release complete message	Retransmit status inquiry message; restart timer T322	Retransmit status inquiry message; restart timer T322

Message Processing

Table 2-4 shows how the router software handles various types of message exchanges.

Table 2-4. Message Processing

Message Type	Message Processing
Call setup	When the software receives a setup message, it performs several validations before it can deliver the message to the called subscriber and return a call proceeding message to the calling subscriber. The software must verify that all of the information fields in the message are in the proper order, all of the mandatory elements are present, and that all elements contain appropriate values.
Call proceeding	After the network determines that the setup message is valid and contains all the appropriate information, it returns a call proceeding message to the calling subscriber. When the network delivers the setup message to the called subscriber, the called subscriber may then return a call proceeding message to the network.
Connect	When the called subscriber accepts a call, it sends a connect message back to the network. The network validates the message and checks any negotiable parameters. If the message passes this inspection, the network passes the message back to the calling subscriber.
Disconnect	When a subscriber wants to terminate a call, it sends a disconnect message to the network. The network validates the messages and passes it to the peer subscriber. The cause information element is mandatory in the disconnect message. Under normal conditions, it contains a value of 16, “Normal Call Clearing.”

(continued)

Table 2-4. Message Processing *(continued)*

Message Type	Message Processing
Release	Under normal call clearing conditions, the network passes the disconnect message through the network to the remote subscriber. The subscriber receiving this disconnect message responds with a release message. The network validates the release message and passes it to the local subscriber.
Release complete	Once the network receives a release message from the subscriber and verifies it, the network returns a release complete message to the subscriber. After receiving the release message from the network, the subscriber responds with a release complete message.

Frame Relay Service Records

Bay Networks uses service records to define frame relay circuits. A *service record* is a data structure that allows flexible grouping and characterization of VCs. A service record can contain a single PVC or SVC, multiple PVCs or SVCs, or a combination of PVCs and SVCs.

Service records:

- Simplify network addressing for VCs because you define and associate only one protocol address with groups of frame relay VCs.
- Allow multiple groups of VCs per frame relay interface.
- Enable you to group multiple VCs for each network protocol into separate service records, thereby reducing the number of buffers needed per circuit during broadcasts.
- Lower customer costs by creating multiple broadcast domains.
- Conserve resources because they require a small number of circuits.
- Are easy to configure.

Default Service Record

The router creates the first service record automatically when you select frame relay as your WAN protocol. This first service record is the *default service record*. Any VCs not associated with another configured service record use the default service record.

Multiple Service Records

Interfaces can have multiple service records, and each service record can contain multiple PVCs, SVCs or combinations of PVCs and SVCs.

Adding and Moving PVCs

You can add PVCs to a service record either individually, or in a range. You can also move PVCs on the same interface from one service record to another individually or as a group. For instructions, see "Customizing PVCs" on page 3-11.

Frame Relay Access Modes

Bay Networks describes frame relay PVCs in terms of three access modes: group, direct, and hybrid. The following topics define each of these modes within the context of service records.

Group Access Mode

Group mode describes a service record with multiple VCs. It represents a true point-to-multipoint circuit. In group access mode, upper-layer protocols treat each frame relay network interface as a single access point to the switched network. The upper-layer protocols use a single network address to send all traffic destined for the switched network to the frame relay network interface.

When you configure each router, you assign only one network address (for example, an IP or IPX address) to the frame relay interface, not to each VC. The Data Link Control Management Interface (DLCMI) dynamically configures VCs on the default service record; you do not need to explicitly configure them.

Service records in group mode:

- Allow multiple groups of PVCs per frame relay connection.
- Enable you to gather multiple VCs for each network protocol into a separate group or service record, thereby reducing the number of buffers needed per circuit during broadcasts.
- Lower customer costs by creating multiple broadcast domains.

Direct Access Mode

Direct mode describes a service record with one PVC. In direct access mode, upper-layer protocols treat the frame relay network as a series of point-to-point connections. The upper-layer protocols view each PVC as an individual network interface.

Service records in direct access mode:

- Limit broadcasts to one PVC.
- Enable multiple layer 3 networks per interface.

Hybrid Access Mode

Hybrid access mode, as its name implies, combines characteristics of group and direct access modes. Frame relay hybrid mode enables you to use the same PVCs for both routing and bridging. It works only for non-fully meshed network configurations that use:

- Both bridging and routing over a single frame relay interface
- Spanning tree bridging

In a *fully meshed* network, PVCs exist between each pair of nodes in the network. In a *non-fully meshed* network, PVCs exist only between nodes that need to communicate. Figure 2-6 shows a non-fully meshed network that uses hybrid mode.

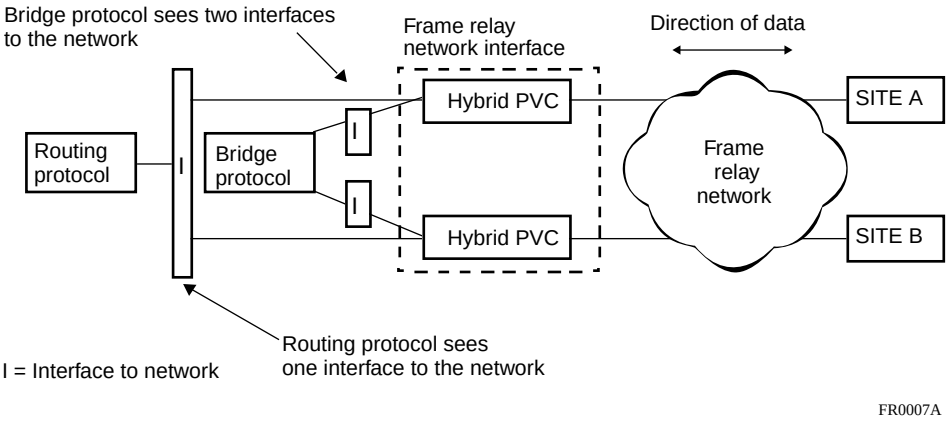

Figure 2-6. Hybrid Mode Configuration, Non-Fully Meshed Network

Using Hybrid Mode for Transparent Bridging

Figure 2-7 shows bridged traffic between site A and site B. The bridge (router 1) is running on the frame relay interface, and its configuration does not use hybrid mode.

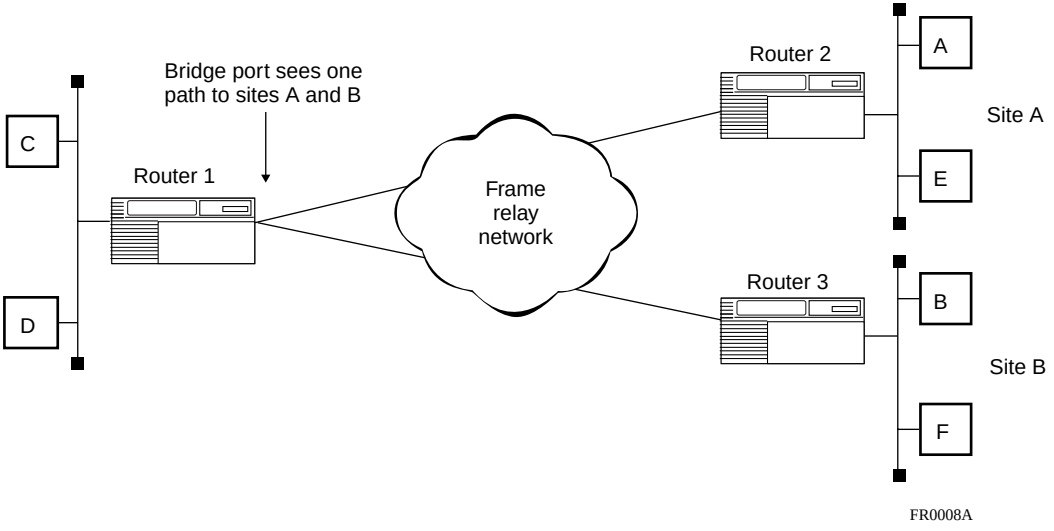

Figure 2-7. Example of a Bridged Network

In this example, the bridge receives data from site A. If the bridge does not recognize the destination address, it tries to direct traffic through another bridge port. However, without hybrid access mode configured, the frame relay bridge port views the paths to site A and site B as the same path. Because the bridge does not send out data on the same port from which it just received data, the bridge does not direct the data to site B. In this case, you should use hybrid access mode.

If you define the PVCs in hybrid mode (see Figure 2-6 on page 2-17), each PVC acts as a separate bridge port. This enables the bridge running on the frame relay interface to view the traffic from site A as arriving on a different port than that of site B. When the bridge sends out data, it sends it out from all ports, including the port that has access to site B. Therefore, data from site A can reach site B.

You configure hybrid mode by enabling the hybrid mode PVC parameter. For instructions, see “Configuring Hybrid Mode for PVCs” on page 3-20.

Source Routing

Source routing is the method by which a bridge sends data across two networks. The router supports source routing over frame relay networks, using RFC 1490 standard frame relay data encapsulation.

To configure source routing, see *Configuring Bridging Services*.

RFC 1490

RFC 1490 defines the encapsulation method for sending data across a frame relay network. Bay Networks routers implement RFC 1490 for all protocols that Bay Networks supports over frame relay networks.

Address Resolution for PVCs

Address resolution for PVCs maps a remote network address such as an IP address to a local DLCI number. For most protocols that you configure for a frame relay interface, the router performs address resolution automatically. However, IP, AppleTalk, and VINES use the Address Resolution Protocol (ARP). ARP dynamically generates an ARP table of addresses and DLCI numbers by sending messages back and forth to each network node to gather address information. This process increases broadcast traffic across the network.

To reduce broadcast traffic for all protocols, you can configure static routes and adjacent hosts at the protocol level. This eliminates the need for the router to perform address resolution. To reduce traffic associated specifically with VINES address resolution, you can configure Inverse ARP. Inverse ARP is the default for IP over frame relay. Refer to the appropriate protocol manual for more information about static routes, adjacent hosts, and Inverse ARP.

Table 2-5 lists how the router handles address resolution for each protocol and whether or not you can reduce broadcast traffic by modifying the address resolution configuration.

Table 2-5. How Protocols Handle Address Resolution

Protocol	How Router Performs Address Resolution	Configuration Requirements
Bridge (including source route)	Automatic	None
IP	ARP or Inverse ARP	Configure ARP Configure Inverse ARP
DECnet IV	Automatic	None
VINES	ARP or Inverse ARP	None for ARP Inverse ARP is the default for frame relay.
Internet Packet Exchange (IPX)	Automatic	None
Xerox Networking System (XNS)	Automatic	None
AppleTalk	AppleTalk ARP	None

Address Resolution for SVCs

For SVCs, adjacent host configuration including either an E.164 or X.121 address eliminates the need for the router to do address resolution.

Traffic Control

Frame relay is unreliable. It does not include error recovery mechanisms, relying instead on the upper layer protocols to detect and retransmit lost frames.

Hub and spoke topologies often present a “big pipe/little pipe” situation. The central or hub site has a faster link to the frame relay service because it is a point of concentration for many remote sites: it has a “big pipe,” with, for example, a T1/E1 connection that can transmit data at rates of 1.54 Mb/s. The remote sites usually support a much lower line speed, 56 Kb/s to 64 Kb/s, or “little pipe.” Figure 2-8 illustrates this concept.

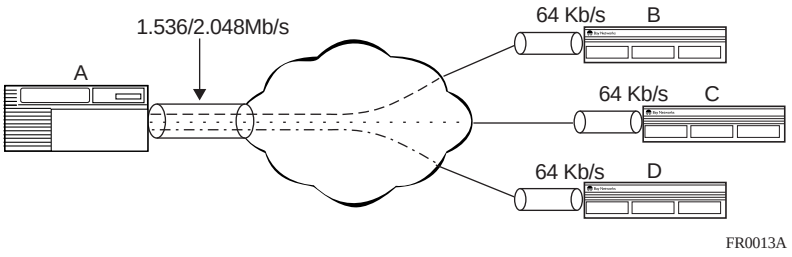

Figure 2-8. Big Pipe/Little Pipe Topology

The central site router sends traffic at its available bandwidth, in this example at T1 rates (1.536 Mb/s in the United States and Canada, 2.048Mb/s elsewhere). Some switches recognize that the remote site is configured at a lower speed, and begin to drop frames above the capacity of the remote site router. At the remote site, the frame relay interface discards frames beyond its available buffer. The assumption is that the user application detects the lost frames and either retransmits them or uses a flow control mechanism in the protocol, such as windowing, to *throttle*, which means queue, the traffic. But not all applications have a robust mechanism to deal with lost or out-of-sequence frames.

You can use Bay Networks WAN Compression Protocol (WCP), protocol prioritization, congestion control, and traffic shaping either singly or in combination to help control the flow of traffic and avoid loss of data.

Data Compression

You can configure both hardware- and software-based data compression over WANs running frame relay.

Enabling compression improves bandwidth efficiency by eliminating redundant strings in data streams. This, in turn, improves network response times and reduces line costs. Enabling compression on a frame relay link also provides reliability. Both sides of a link using compression maintain a history of data that has already traveled across the network, and WCP (WAN Compression Protocol) detects and retransmits dropped packets.

To use data compression with frame relay, the Compression Control attribute or parameter must be set to Enable, the default value (see “Enabling Compression for PVCs” on page 3-32 for information about how to access this attribute or parameter). You must also select WCP from the protocols menu.

For a complete discussion of data compression, see *Configuring Data Compression Services*.

Data Encryption

Bay Networks data encryption services enable you to protect sensitive traffic on your network. Encryption for frame relay circuits works with direct mode PVCs only. For information about and instructions for configuring data encryption, see *Configuring Data Encryption Services.*

Protocol Prioritization

You can set priorities for the traffic sent across a synchronous line interface using a process called *protocol prioritization*. The ability to prioritize traffic is important for an application that is time-sensitive and that requires a fast response.

For example, a user at router A participating in a Telnet session with router B requires a more immediate response than does a user at router A performing a file transfer with router B.

When you select frame relay on a circuit, the router enables protocol prioritization automatically. It does so because the DLCMI packets must have a higher priority than any other packets you are sending across the network.

For more information about protocol prioritization, see *Configuring Traffic Filters and Protocol Prioritization.*

Congestion Control

Network congestion can degrade network performance. Congestion occurs when a node receives more frames than it can process, or sends more frames than the transmission line can handle. The frame relay network informs the nodes of congestion, so that they can reduce the amount of traffic across the network.

In the frame relay packet header, there are two bits that the network sets to alert nodes of network congestion. These bits, as defined by the frame relay specification, are the forward explicit congestion notation (FECN) bit and the backward explicit congestion notation (BECN) bit.

If the network detects congestion, it alerts the router in the same direction as the received frame by changing the frame's FECN bit from 0 to 1. For nodes in the opposite direction of the received frame, it changes the frame's BECN bit from 0 to 1 (Figure 2-9).

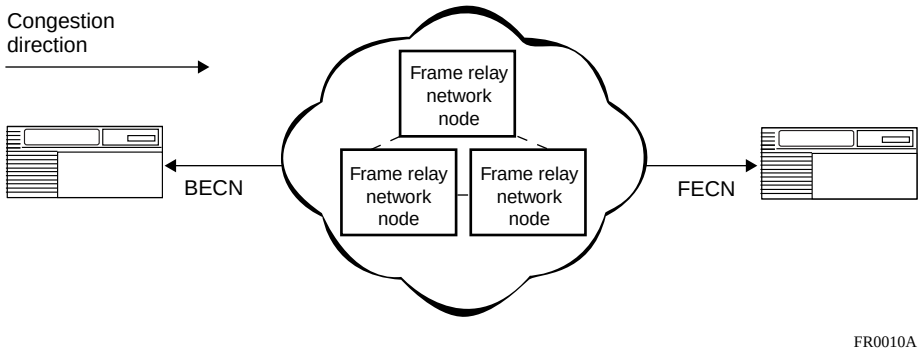

Figure 2-9. Detecting and Controlling Network Congestion

If you enable the congestion control feature, you can specify the number of FECN/BECN bits the router receives in a given time period before it stops transmitting frames. While frames are going across the network, the frame relay interface checks received packets for FECN and BECN bits set to 1. If the interface receives the specified number of bits during the designated time period, frame relay drops all traffic destined for the PVC where there is congestion. When the interface no longer receives these congestion notifications, the router resumes transmission.

For example, suppose you set the congestion timer to 0.5 second and the congestion count to 3. In this case, if an interface receives 3 FECNs or BECNs within 0.5 second, the node stops sending frames (although it continues to receive frames for this PVC). If the interface receives no FECNs or BECNs during the next 0.5 second, the router resumes transmission. For instructions on configuring the congestion attributes or parameters, see “Controlling Congestion for PVCs” on page 3-22 and “Controlling Congestion for SVCs” on page 3-58.

If you enable congestion control and also enable traffic shaping, you can throttle, which means queue, congested traffic rather than drop it by choosing the value, *Throttle*, in the Congestion Method attribute or parameter (for a description of the Congestion Method parameter, see page A-11).

Traffic Shaping

Traffic shaping relieves bottlenecks in topologies with high-speed connections to the central site, and low-speed connections at remote sites (as in Figure 2-8 on page 2-20). Committed information rate enforcement and quality of service are the major components of Bay Networks traffic shaping.

Committed Information Rate

The *committed information rate* (CIR) is the rate at which the network supports data transfer under normal operations. Its name is descriptive: you have a contract with your carrier, who has *committed* to providing a given *throughput*, here called the committed information rate. The CIR is measured in bits per second. You configure this value that the carrier provides per virtual circuit.

CIR of 0

You can contract with a carrier for a CIR of 0, which yields best-effort service at low cost. The carrier transmits data, but does not commit to providing a specified throughput. To configure a CIR of 0, set both the Throughput attribute or parameter (which is the CIR) and the Committed Burst (B_c) attribute or parameter to 0, and set the Excess Burst (B_e) attribute or parameter to a value greater than 0. For more information on burst rates, see "Committed Burst Rate and Excess Burst Rate" on page 2-24.

Maximum CIR

The maximum CIR should not be greater than the speed of the access line on the slower end of a virtual circuit. In a big pipe/little pipe topology (illustrated in Figure 2-8), likely CIRs at the remote sites would be 32 Kb/s, 56 Kb/s, or 64 Kb/s. If you configure CIRs for these virtual circuits at the central site, you can use CIR enforcement (described in the next topic) to prevent the big pipe from sending traffic that exceeds the PVC CIRs.

CIR Enforcement

CIR enforcement means restricting the speed of outbound traffic to a rate no faster than the CIR. It is the major component of traffic shaping. You can configure CIR enforcement to operate over Synchronous, High-Speed Serial Interface (HSSI), T1, E1, and Integrated Services Digital Network (ISDN) lines, for frame relay backup, demand, bandwidth-on-demand, and leased lines at the virtual circuit level. CIR enforcement operates on whole frames only. It controls congestion either by bringing down the virtual circuit, or by queuing the traffic, which is also called *throttling*.

Committed Burst Rate and Excess Burst Rate

The *committed burst rate* (B_c) defines the number of bits that the router can transmit over a specified time interval (T_c) when congestion is occurring. The *excess burst* (B_e) defines the number of extra bits that the router attempts to send over the T_c when there is no congestion. Both the B_c and the B_e are values that you configure.

The sum of the B_c and the B_e is the maximum amount of traffic that can travel across the network per T_c when there is no congestion. If you set the B_e to a value greater than zero, the router can send traffic exceeding the CIR. To enforce the CIR, that is, to limit traffic that the router can send to the amount of the CIR, set the B_e to 0.

If you enable congestion control *and* set the congestion method to throttle, the virtual circuit sends only B_c bits of data over the time interval T_c when congestion occurs, even if you have configured the B_e to a value greater than 0. It queues the excess data until congestion abates. If you set the congestion method to throttle-then-shutdown, the virtual circuit first queues traffic when congestion occurs, and then terminates the virtual circuit if throttling does not alleviate congestion.

Quality of Service

Quality of Service (QoS) is the second major component of Bay Networks traffic shaping. It uses protocol prioritization with traffic shaping. You configure a prioritization filter on the default service record for the entire frame relay interface, and CIR enforcement per virtual circuit (VC). QoS operates over Synchronous, HSSI, T1, E1, and ISDN lines, for backup, demand, and for leased lines. Although the HSSI driver does not support protocol prioritization, VCs on an HSSI interface do.

Using protocol prioritization with traffic shaping creates two levels of queues. For traffic shaping the queues are high/normal/low at the VC level. For protocol prioritization they are interrupt/shaping/high/normal/low at the driver level. Figure 2-10 illustrates this concept.

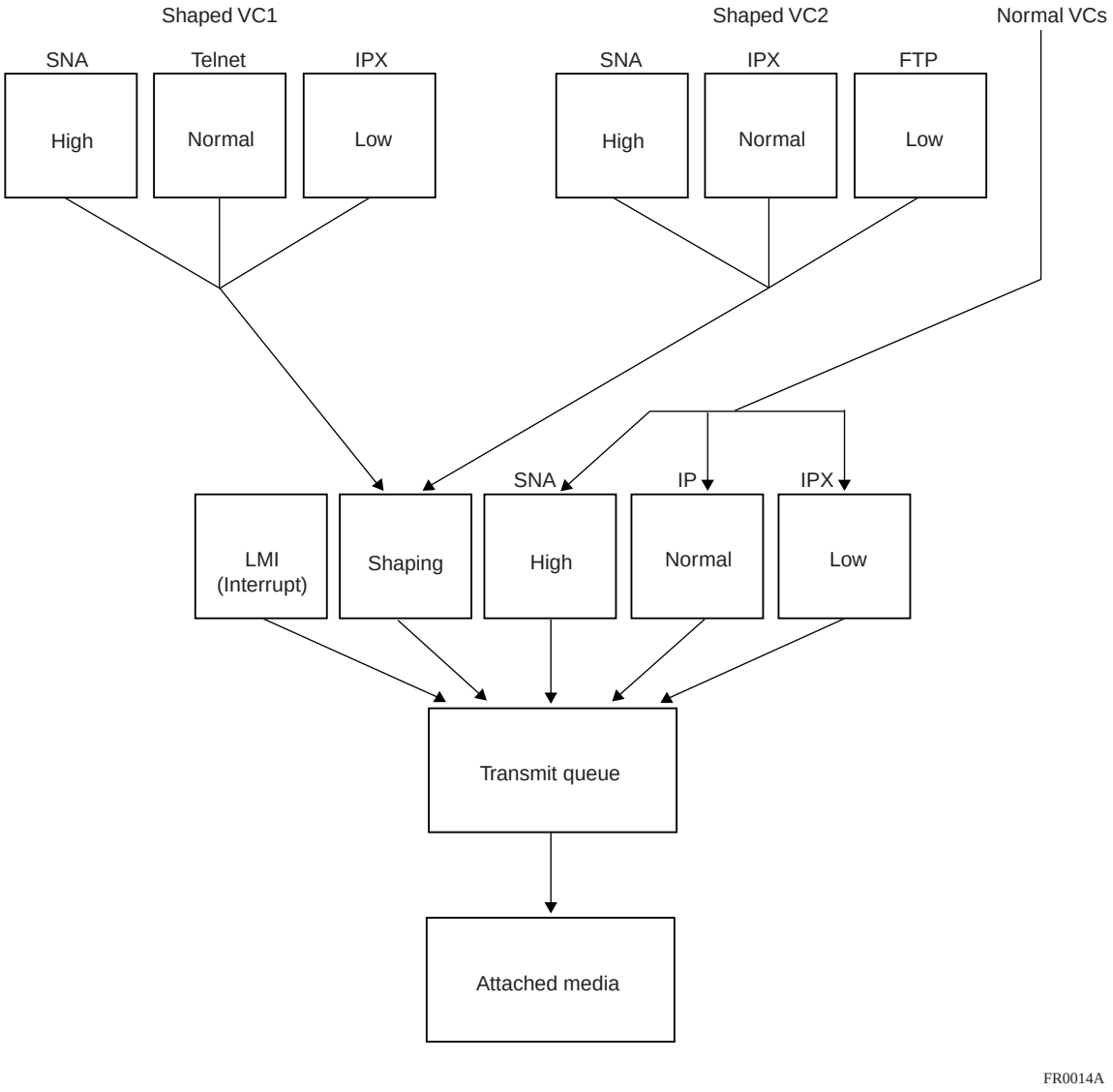

Figure 2-10. Traffic Shaping Queues

All traffic that goes to a traffic-shaped VC (VC1 or VC2) is queued as high, normal, or low priority at the VC level, and then it travels, by priority order, to a shaping queue within the driver. Normal VC traffic is queued as high, normal, or low priority at the driver level. At the driver level:

- Interrupt priority traffic, DLCMI/LMI requests (the LMI box in Figure 2-10), has the highest priority. You cannot change this.
- Shaped priority traffic (the Shaping box in Figure 2-10) has the second highest priority.
- Normal VC traffic (not shaped) has lower priority than shaped traffic. You can still prioritize normal VC traffic as high, normal, or low.

Queuing and prioritization only matter when the traffic rate exceeds the VC line rate or the CIR. If the total of all traffic is below the CIR, the router just transmits it.

You cannot prioritize between VCs on which you have enabled traffic shaping. The router schedules traffic among them in a round-robin manner.

For information about configuring filters for protocol prioritization, see *Configuring Traffic Filters and Protocol Prioritization.*

Traffic Shaping for SVCs

Traffic shaping for SVCs works according to the descriptions in the previous topics, except that SVCs derive the committed burst, excess burst, and throughput values from a combination of the traffic shaping attributes and parameters that you configure, and values that the frame relay network imposes. The network values are called *link layer core (LL Core) values*,

Requesting Quality of Service for SVCs

When you configure traffic shaping for an SVC, you have several alternatives to achieve the QoS that will best serve your network:

- You can set the SVC Traffic Shaping Disable attribute or parameter to Enable without providing values for the traffic shaping attribute or parameters. The SVCs you configure in this way use LL Core values that the network provides.

- You can set the SVC Traffic Shaping Disable attribute or parameter to Enable, and provide values for the LL Core traffic shaping attribute or parameters.

  If you supply values for the LL Core attribute or parameters, the router requests an SVC from the frame relay network with the quality of service you have designed. However, the router can only request the values you have configured. The actual values the network supplies may be less than requested because the local router, the network, and the remote end negotiate the actual quality of service. To track the values an SVC uses, use the Site Manager Statistics Manager (for more information, see *Configuring and Managing Routers with Site Manager*).

- You can set the SVC Traffic Shaping Disable attribute or parameter to Disable, and provide values for the LL Core Committed Burst, Excess Burst and Throughput attribute or parameters.

  If you configure traffic shaping this way, the router does not enforce the CIR it requests from the frame relay network. There is a risk of oversubscribing the interface, which may result in dropped packets.

Refining Quality of Service for SVCs

SVCs allow you to refine quality of service requirements in that you can specify values for traffic shaping attribute or parameters for both incoming and outgoing directions, and you can set values for incoming and outgoing minimum acceptable throughput.

The values you set in *incoming* and *outgoing* attribute or parameters apply to traffic depending on where the SVC call originates. See “Defining Incoming and Outgoing” on page 2-29 to understand how the software uses these attribute or parameters.

Refining Traffic Shaping

The attribute or parameters involved are the LL Core Out Throughput (CIR), LL Core Out Committed Burst, LL Core Out Excess Burst, LL Core In Throughput (CIR), LL Core In Committed Burst, and LL Core In Excess Burst. You can use these attribute or parameters to request values for traffic shaping that distinguish between incoming and outgoing traffic.

Setting Minimum Acceptable Throughput

Throughput that an SVC actually uses may be less than it requests because the local router, the frame relay network, and the remote end of the connection negotiate QoS. You can use the Outgoing and Incoming Minimum Acceptable Throughput attributes or parameters to set the lowest throughput value the router will accept. If either the local router, the network, or the remote end cannot guarantee that value, the SVC will not be established.

Defining *Incoming* and *Outgoing*

If a local router originates the call, the outgoing committed burst, excess burst, and throughput values define characteristics of data the local router transmits, while the incoming values define characteristics of data the local router receives. If the local router receives a call, the outgoing values define characteristics of data the local router receives, while incoming values define characteristics of data the local router transmits. Table 2-6 explains this further.

Table 2-6. Incoming and Outgoing

Call Originator	Direction of Data	Attribute or Parameter Values that Apply
Local router	Outgoing to remote router	Outgoing
	Incoming from remote router	Incoming
Remote router	Incoming to local router	Outgoing
	Outgoing from local router	Incoming

Traffic Shaping Considerations

Traffic shaping is best used at central offices to prevent the “big pipe” from sending too much data too quickly to remote sites with “little pipes.” Let this principle guide your decisions about how to use traffic shaping on your network.

CIR Configuration Guidelines

Consider the following when you configure traffic shaping.

- In general, the value you assign to the B_c should equal 1/4 of the CIR to avoid excessive queuing and dropped packets.
- If, however, you are sending frames that exceed the size of the B_c, data travels very slowly because the router must use multiple time periods to accommodate the packet size and avoid exceeding the CIR. If setting the B_c to 1/4 of the CIR yields a value lower than packet size, set the B_c to 1/3 or even 1/2 of the CIR.

  For example, a typical TFTP frame is 548 bytes. If the CIR is 16,000 bits, the B_c configured according to the 1/4 guideline would be 4,000 bits, or 500 bytes, which is not big enough to accommodate a TFTP frame. If you set the B_c to 16,000/2, or 1/2 CIR, the result is 8,000 bits, or a packet size of 1,000 bytes, which works, but may result in excessive queuing because the T_c is 1/2 second. If you set the B_c to 16,000/3 or 1/3 of CIR, the result is a B_c of 5,333 bits or 666 bytes, much closer to the 548 TFTP frame size.
- If you cannot predict the typical frame size, monitor frame relay shaping statistics for numbers of large frames and dropped frames. If either of these numbers is increasing constantly or dramatically, adjust the B_c to a higher value in small increments.

WCP and CIR Enforcement

Consider the following when you are determining the best configuration for your network:

- Data compression maximizes throughput and increases reliability.
- Traffic shaping increases reliability, controls congestion, and prioritizes traffic.
- Compression and traffic shaping together maximize reliability, but at the expense of throughput.

Using Traffic Shaping with Data Compression

Traffic shaping occurs at the VC level; compression, at the driver level. Shaping therefore occurs before compression, which compromises effective compression because only the precompressed traffic is shaped: the compressed traffic is not shaped. WCP compresses data at the rate it receives it, which with traffic shaping is the CIR. It is therefore unrealistic to expect a high compression throughput for data that originates from a site that also uses traffic shaping.

Using Traffic Shaping Effectively

You can use traffic shaping at one or both ends of a link, but you must use compression at both ends of a link. It makes sense to use traffic shaping at a central site, where you have a T1 line that sends data to remote sites with 64 KB line rates, and the goal is to control the flow of traffic and avoid flooding the remote sites. But if the CIR is equal to the line rate, which could well be the case at the remote site with 64 KB line rates, there is no need to use traffic shaping.

Using Compression Effectively

You can use compression effectively in the case of the 64 KB site which does not use traffic shaping. You can also compensate for the throughput cost associated with using compression and traffic shaping at the central site by taking into account characteristics of compression and traffic shaping, and fine-tuning traffic shaping parameters.

- When you configure traffic shaping, take into account the compression ratio you want to achieve.
- If you set the B_e equal to the B_c, the router doubles the amount of traffic it attempts to send and, when you enable compression, compresses that amount of traffic, because WCP compresses data at the rate it receives it.
- If you also set the Congestion Method parameter to throttle, the router will queue traffic if congestion occurs, and thus prevent exceeding the CIR.
- Congestion may occur if compression histories are not in sync, and WCP has to resend packets. If WCP retransmits many packets, it may exceed the CIR.

Oversubscribing the Interface

The CIRs that you configure are based on an average peak rate for the VCs on the network. If all VCs with traffic shaping try to send data simultaneously, they may exceed the capacity of the interface. If you oversubscribe the interface, traffic shaping will still enforce the CIR, but there may be additional latency for reserved flows. VCs without traffic shaping will send data after traffic shaped VCs.

Queue Limits and Data Clipping

Bay Networks routers maintain buffers for each traffic shaped VC. Each buffer can hold one frame that the router cannot send because of congestion. The router divides the number of buffers on the interface. Some key facts specific to buffers are:

- The default number of buffers is 200 per interface. To change the buffer number, you can use the Technician Interface.
- The software divides the number of buffers on the interface by the number of traffic-shaped VCs, giving each VC the same number of buffers. Therefore, if you have 10 traffic-shaped VCs per interface, each VC has 20 buffers.
- If you enable protocol prioritization, the default number of buffers is 30 for high priority traffic, 200 for normal, and 30 for low.

You can use the Technician Interface to increase the total number of buffers for the interface, and you can also redistribute buffers among the VCs and among priority queues.

The parameters that you customize at the interface level are:

- wfFrDlcmiShapingHiQueueLimit
- wfFrDlcmiShapingNormalQueueLimit
- wfFrDlcmiShapingLoQueueLimit

The parameters you can customize at the VC level are:

- wfFrCircuitShapedHiQueueLimit.
- wfFrCircuitShapedNormalQueueLimit
- wfFrCircuitShapedLoQueueLimit

For information on using the Technician Interface, see *Using Technician Interface Software.*

FECN and BECN Notification Bits

The topic "Congestion Control" on page 2-22 explains that a specified number of FECN and BECN bits received during a set time period indicate congestion. When congestion occurs on a traffic shaped VC, the router either drops traffic, throttles it, or throttles and then drops traffic, depending on the value of the Congestion Method attribute or parameter.

The FECN and BECN notifications are part of the header in a frame relay data packet. In a big pipe/little pipe topology (see Figure 2-11), the central site router A typically sends much more data than it receives. This means that the remote site routers B, C, and D that receive a lot of traffic may be getting large numbers of FECNs, while the central site router is getting relatively few data packets, and therefore few BECNs, and is unaware than congestion is occurring. You may need to fine tune the Congestion Counter parameter and the Congestion Timer parameter (see Appendix A, "Site Manager Parameters"), from the default values of 20 FECN or BECN counts per second to, for example, 10 counts per 5 seconds to account for the differences in traffic volume from and to the central site.

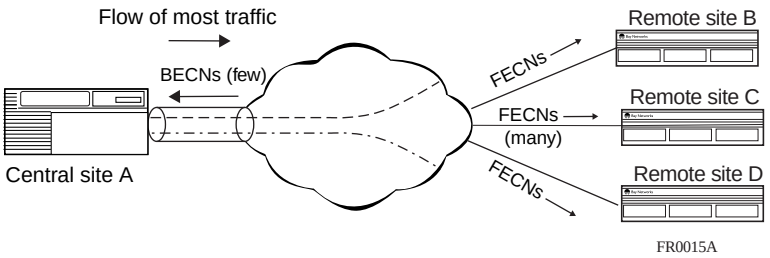

Figure 2-11. FECNs and BECNs in Big Pipe/Little Pipe Topology

X.213 Priority for SVCs

Some frame relay networks that support SVCs can prioritize SVC data and connection characters by setting X.213 priority attribute or parameters. You configure values for these attributes or parameters at the router, and the frame relay network uses them. For instructions on configuring X.213 parameters see “Setting X.213 Priorities for SVCs” on page 3-71.

Inactivity Timing for SVCs

The Inactivity Timer parameter and Inactivity Timer Mode parameter combine to automatically disconnect an SVC according to values that you configure for amount of time and the direction that data is flowing over the SVC. You can configure these parameters to apply to all SVCs in a service record, and you can also configure them for individual SVCs.

When the router establishes an SVC, the Inactivity Timer value initializes two timers internal to the router: the one that monitors data the router transmits, and one that monitors data the router receives. The Inactivity Timer Mode parameter defines how the timers restart. Table 2-7 shows the various ways you can set these parameters, and the effect each combination has on disconnecting SVCs.

Table 2-7. Inactivity Timer and Inactivity Timer Mode Interaction

Inactivity Timer Mode	Inactivity Timers Used	Disconnect SVC
Both Directions	Transmit and Receive	When both timers expire (no data transmitted, AND no data received during the timer interval).
Either Direction	Transmit and Receive	When either timer expires (no data transmitted OR no data received during the timer interval).
Transmit Only	Transmit	When the transmit timer expires (no data transmitted during the timer interval).
Receive Only	Receive	When the receive timer expires (no data received during the timer interval).

For instructions on setting these values for the inactivity parameters, see “Setting Inactivity Values for SVCs” on page 3-55.

Transmit Inactivity Timer and Protocol Priority No-Reset Filter

A Protocol Priority filter with a No-Reset action affects the operation of the timer that monitors data the router transmits. Normally this timer restarts for timer modes *Both*, *Either*, or *Transmit Only*. But data the router transmits over an SVC that matches a Protocol Priority filter with a No-Reset action does not restart the transmit inactivity timer. This may cause the SVC to disconnect even though it is transmitting data.

Managing Routing Information Protocol (RIP) Over SVCs

RIP is a mechanism that IP and IPX use to inform network entities of routing topology changes. The IP and IPX protocols allow you various controls over the frequency and destination of RIP packets. Because RIP packets can affect how the router establishes and disconnects frame relay SVCs, the software has controls that apply to how RIP interacts with the frame relay SVC Inactivity Timer parameter and the Inactivity Timer Mode parameter. For more information, see Appendix B, "RIP Management for Frame Relay SVCs."

Multiline for PVCs

Frame relay provides a link redundancy feature called multiline, which works with frame relay PVCs. *Multiline* is a Bay Networks proprietary implementation that lets you group two or more physical lines that back each other up in case of a failure. This ensures that information arrives at its destination on the network. In addition, if both lines are up, the router uses both lines simultaneously. Two or more physical lines must be available for a multiline configuration. Figure 2-12 illustrates a multiline configuration.

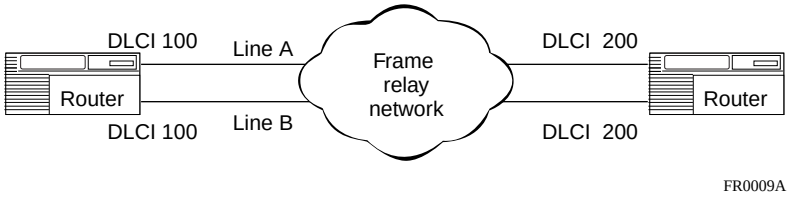

Figure 2-12. Multiline Network

In this example, when the router receives traffic destined for the network, it alternates or randomizes (depending on how you configure it) between line A and line B to transmit the data. The router uses both lines simultaneously to balance the traffic between each path. If one of these lines goes down, the router uses the remaining line.

You can create a multiline configuration of up to four service records. Each service record must be on a different physical line on the router. Each line should be on a different slot to provide fault tolerance.

You must also match DLCIs in each service record of the multiline. Matching DLCIs ensures that a backup exists for each PVC.

The most important part of configuring multiline is setting the PVC DLCI number. This number identifies each PVC, thereby specifying a path for the router to direct data to the network. For each frame relay PVC that you configure, check that PVCs with the same destination have the same DLCI number.

Note: If you use multiline, packets traveling on the two paths may arrive at their destination out of sequence. Some protocols do not tolerate packets arriving out of sequence and, as a result, you may experience poor performance or failures.

For more instruction on configuring multiline mode, see “Grouping Service Records for Multiline Mode” on page 3-34.

Traffic Distribution Between Data Paths

To distribute traffic between multiline data paths, you can use one of two methods:

- Random distribution
- Address-based distribution

Random Distribution

Random distribution means that as the router sends out each packet, it alternates between the lines. This option determines which line the packet uses based on a randomly assigned number. For each outbound packet, the router generates a random number, and this number designates the line to use.

Random balancing evenly distributes traffic and lets the router use the two lines efficiently. Because packets travel on different paths, they arrive at the destination out of sequence, and the upper-layer protocols, for example, IP and Open Systems Interconnection (OSI), have to resequence the information. Some protocols cannot tolerate packets arriving out of sequence, so be sure this option is appropriate for your application.

Address-Based Distribution

Address-based distribution determines the data path for outbound traffic from the source and destination address in each packet. Any given address pair always uses the same path.

The router determines whether to route or bridge the packet, and then uses the corresponding level of address. It uses routing-level addresses for routing traffic, and the MAC-level addresses for bridging traffic.

Address-based distribution ensures that all outbound traffic travels on the same path, and that packets arrive in sequence. For protocols that cannot receive packets out of sequence, use this method. Note, however, that this option does not always distribute traffic evenly across each line.

Protocol Prioritization and Multiline Incompatibility

You cannot use protocol prioritization with multiline. Protocol prioritization may change the order of frames arriving over a multiline interface, and frame relay multiline does not have the ability to correct the sequence.

PVC Pass-Through

The *PVC pass-through* service allows a single frame relay network access link to carry both conventional network protocol traffic, and otherwise unroutable frame relay access device (FRAD) traffic. It works with hybrid mode PVCs only. PVC pass-through connects two PVCs on separate interfaces so that the router can transmit traffic it receives on one PVC out the other with no encapsulation requirements. Figure 2-13 illustrates how PVC pass-through works.

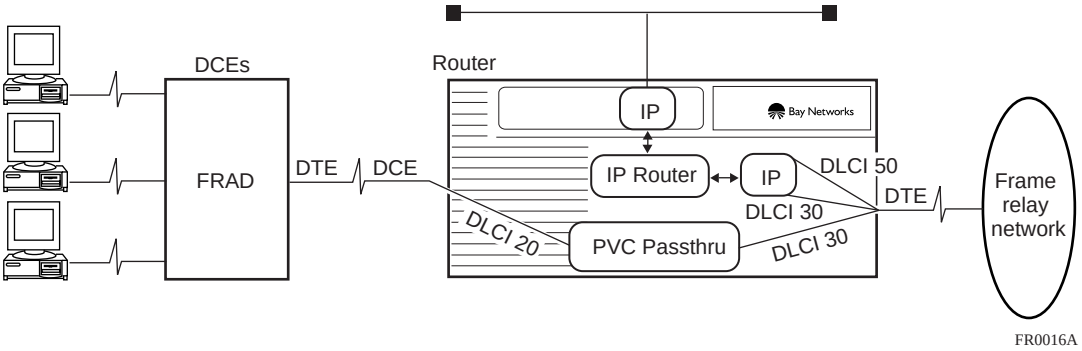

Figure 2-13. PVC Pass-Through

Figure 2-13 shows a router with an Ethernet interface, and two frame relay interfaces. The frame relay interface to the frame relay network is a DTE (right side of illustration). The frame relay interface to the FRAD is a DCE (left side). The router delivers all IP frames inbound on DLCI 50 to the IP interface. It also delivers all IP frames inbound on DLCI 30 to the IP interface. The router delivers all other traffic inbound on DLCI 30 via the PVC pass-through system to DLCI 20, which transmits the data to the FRAD. All data inbound on DLCI 20 is delivered via the PVC pass-through system to DLCI 30, which transmits the data to the frame relay network.

PVC pass-through works with both leased line and dial-on-demand interfaces. It works with Bay Networks data compression, congestion control, and traffic shaping. It does not work with data encryption, which requires a direct mode PVC.

Frame Relay Dial Services

Frame relay works with Bay Networks dial-on-demand and dial backup services. For information about and directions for configuring dial services see *Configuring Dial Service*s.

Configuring Synchronous Lines for Frame Relay

If you enable frame relay on a circuit, Site Manager automatically sets the following synchronous line parameters (Table 2-8):

Table 2-8. Synchronous Line Parameters for Frame Relay

Parameter	Value
BofL	Disable
Promiscuous	Enable
Service	Transparent
WAN Protocol	Frame Relay

For more information on these parameters, refer to *Configuring WAN Line Services*.

For More Information About Frame Relay

For more information about frame relay, consult the following documents:

American National Standards Institute, T1.617-1991. *Integrated Services Digital Network (ISDN) – Digital Subscriber Signalling System No. 1 (DSS1) - Signalling Specification for Frame Relay Bearer Service.* Washington, D.C., June 1991.

-- T1.617 Annex D-1991. *Additional Procedures for Permanent Virtual Connections (PVCs) Using Unnumbered Information Frames.* Washington, D.C., June 1991.

-- T1.618-1991. *Integrated Services Digital Network (ISDN) - Core Aspects of Frame Protocol with Frame Relay Bearer Service.* Washington, D.C., June 1991.

Bradley, T., C. Brown, and A. Malis. *Multiprotocol Interconnect over Frame Relay. RFC 1490.* Menlo Park, California: Network Information Center (NIC), SRI International, January 1992.

Digital Equipment Corporation et al. *T1S1 - Standards based Frame Relay Specification with Common Enhancements.* Document Number 001-208966, Revision 1.0, September 1990.

FRF.4, *Frame Relay User-to-Network SVC Implementation Agreement*, January 5, 1994, plus Attachments A and B to FRF.4.

ITU-T Recommendation Q.933, *Digital Subscriber Signalling Specification No. 1 (DSS 1) - Signalling Specification for Frame Mode Basic Call Control*, October 1995.

ITU-T Recommendation Q.931, *Digital Subscriber Signalling System No. 1 (DSS 1) - ISDN User-Network Interface Layer 3 Specification for Basic Call Control*, March 1993.

ITU-T Recommendation Q.922, *Digital Subscriber Signaling Specification No. 1 (DSS 1) - Data Link Layer - ISDN Data Link Layer Specification for Frame Mode Bearer Services*, 1992.

The following publications provide a less technical introduction to frame relay:

Davidson, R., and N. Muller. *The Guide to SONET: Planning, Installing & Maintaining Broadband Networks.* New York: Telecom Library, Inc., 1991.

Goldstein, F. *ISDN in Perspective.* Reading, MA: Addison-Wesley, 1992.

Jennings, E., T. Jones, and K. Rehbehn. *The Buyer's Guide to Frame Relay Networking.* Netrix Corporation.

Chapter 3
Customizing Frame Relay

When you enable frame relay, default values are in effect for all Bay Command Console (BCC) attributes and Site Manager parameters (for Site Manager parameter descriptions, see Appendix A, “Site Manager Parameters”). Depending on your network requirements, you may want to change these values. The following sections describe how to customize frame relay for your network.

Topic	Page
Using the MIB Object ID	3-1
Selecting a Management Type	3-2
Selecting Address Type and Length	3-4
Monitoring the Connection	3-6
Customizing PVCs	3-11
Customizing SVCs	3-35
Deleting Frame Relay	3-74

Using the MIB Object ID

The Technician Interface allows you to modify attributes by issuing **set** and **commit** commands with the MIB Object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.

Caution: The Technician Interface does not verify attribute values you enter. Entering an invalid value can corrupt your configuration.

Selecting a Management Type

You can specify the management protocol that the router and the frame relay network use to communicate status information. Routers connected back to back also use a management protocol to exchange status information. The following list describes your options:

- *DLCMI None* provides no management interface between the router and the frame relay network. In the absence of management support, you must configure all PVCs manually.
- *Rev 1 LMI* provides user-side management services as specified by Revision 1 of the Local Management Interface standard.
- *ANSI T1.617D* provides user-side management services as specified in Annex D to ANSI standard T1.617-1991. This is the default value.
- *CCITT Annex A* provides user-side management services as specified by the ITU-T (formerly CCITT).
- *LMI Switch* offers limited management services for the DCE side of the connection as specified by Revision 1 of the Local Management Interface standard.
- *Annex D Switch* provides limited management services for the DCE side of the connection as specified in Annex D to ANSI standard T1.617-1991.
- *Annex A Switch* provides limited management services for the DCE side of the connection as specified by the ITU-T.

If you are connecting two routers back to back, use one of the DTE parameter options (Rev 1 LMI, ANSI T1.617D, CCITT Annex A) for the router acting as a DTE, and one of the DCE options (LMI Switch, Annex D Switch, Annex A Switch) for the router acting as the DCE. Although you can configure the router for the DCE side of a connection, the router cannot act as a full switch, and it will not perform complete bidirectional signaling.

The LMI Switch, Annex D Switch, and Annex A Switch options are primarily for troubleshooting.

You can use either the BCC or Site Manager to select a management type.

Using the BCC

To specify a management protocol:

1. **Navigate to the dlcmi prompt.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2; dlcmi
   ```

2. **Enter the management-type command and the value you want the network to use.**

   management-type <*value*>

   The legal values are:

   none
   lmi
   annex-d (the default)
   annex-a
   lmi-switch
   annex-d-switch
   annex-a-switch

   For example, the following command line changes the management type from Annex D Switch to LMI Switch:

   ```
   dlcmi/1/2# management-type lmi-switch
   dlcmi/1/2#
   ```

Using Site Manager

To specify a management protocol:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Interfaces**.	The Frame Relay Interfaces window opens.
4. Set the **Mgmnt Type** parameter. See **Help** or the parameter description on page A-5.	

Site Manager Procedure *(continued)*	
You do this	**System responds**
5. Edit other parameters if you want, and click on **Apply**.	
6. Click on **Done**.	You return to the main Configuration Manager window.

Selecting Address Type and Length

You can specify the data link connection identifier (DLCI) address type and length that the router and the frame relay network use to direct packets to their destinations. The address type for the router and for the switch must be the same.

Selecting a DLCI Address Type

The options for the DLCI address type parameter are:

- *ADDR Q922* selects addressing as specified in the final version of the Q.922 standard. Q.922 provides for FECN, BECN, DE, and EA bits. While most Q.922 addresses are included within a 2-octet field, the standard allows for 3- and 4-octet address fields. This is the default.
- The *November draft of ADDR Q922* differs from ADDR Q922 in dropping the D/C bit from the extended (3- and 4-byte) forms. The D/C bit (DLCI or DL-Core Control Indication) is always 0.
- The *March draft of ADDR Q922* differs from ADDR Q922 in defining an 11-bit DLCI and dropping the DE bit from the second octet of the address field.
- *ADDR Q921* differs from ADDR Q922 MARCH 90 in that it does not use FECNs or BECNs, which means that it does not provide congestion control.

Selecting Address Length

The options for the DLCI address length are 2, 3, or 4 bytes. To understand the distinctions among these byte formats, see the illustrations of frame relay headers in Figure 2-2 and Figure 2-3 on page 2-6.

You can use either the BCC or Site Manager to configure address type and length.

Using the BCC

To specify address type and length:

Address Type

To specify the address type:

1. **Navigate to the frame-relay prompt.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2
   ```

2. **Enter the address-type command and the value you want the network to use.**

   address-type *<value>*

   The legal values are:

   q922-march
   q922-november
   q921
   q922march90
   q922november90
   q922 (the default)

   For example, the following command line sets the address type to q921:

   ```
   frame-relay/1/2# address-type q921
   frame-relay/1/2#
   ```

Address Length

To specify the address length:

1. **Navigate to the frame-relay prompt.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2
   ```

2. **Enter the address-length command and the value you want the network to use.**

   address-length *<integer>*

   <integer> is a value of 2, 3, or 4 (bytes).

For example, the following command line sets the address length to 4 bytes:

```
frame-relay/1/2# address-length 4
frame-relay/1/2#
```

Using Site Manager

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Interfaces**.	The Frame Relay Interfaces window opens.
4. Set the following parameters, using **Help** or the parameter descriptions on page A-6: • **Address** • **Address Length**	
5. Edit other parameters if you want, and click on **Apply**.	
6. Click on **Done**.	You return to the main Configuration Manager window.

Monitoring the Connection

You can monitor the status of your frame relay network connection by setting:

- *Time intervals* for the router to send messages that verify the integrity of the link
- *The number and frequency of error messages* that can occur before the connection terminates

Polling Interval

The *polling interval* specifies the interval between status inquiry messages that the router transmits. Status inquiry messages cause a network response in the form of a link integrity verification message or full status message. Successful completion of the request/response “handshake” verifies the status of the router/frame relay network link. You should accept the default value, 10 seconds. If this value does not match what the network requests, enter a value that is appropriate for your network in the range of 5 to 30 seconds. The polling interval does not function if you set the Management (Mgmnt) Type parameter to DLCMI None.

Full Enquiry Interval

The *full enquiry interval* specifies the interval between full status inquiry messages that the router transmits. Full status inquiry messages cause the network to send a full status report message, which lists all PVCs and their status (active or inactive, and new or previously established).

The default value, 6, tells the router to send a full status inquiry every 6 polling intervals. For example, with a polling interval of 10 and a full enquiry interval of 6, the router transmits a full status inquiry every 60 seconds. With a polling interval of 20 and a full enquiry interval of 30, the router transmits a full status inquiry every 10 minutes (600 seconds). The full enquiry interval does not function if you set the Mgmnt Type parameter to DLCMI None.

Error Threshold and Monitored Events

Error threshold and monitored events together establish a criterion to evaluate the quality of the router’s frame relay network connection. The *error threshold* is the number of faulty status messages that must occur to terminate the connection. *Monitored events* is the number of status message exchanges, within which number those errors occur.

For example, if you accept the default of 3 for the error threshold, and the default of 4 for monitored events, three status exchange errors in a sequence of four attempted exchanges brings the connection down. Similarly, if you set error threshold to 5 and monitored events to 10, five status exchange errors in a continuous sequence of 10 attempted exchanges brings the connection down.

Note: The Error Threshold parameter and Monitored Events parameters do not function if you set Mgmnt Type to DLCMI None.

You can use either the BCC or Site Manager to specify error threshold and monitored events.

Using the BCC

To specify error threshold and monitored event values, use these instructions:

Polling Interval

To set the polling interval:

1. **Navigate to the dlcmi prompt.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2; dlcmi
   ```

2. **Enter the polling-interval command and the value you want the network to use.**

   polling-interval *<integer>*

   <integer> is the polling interval in seconds; the legal values are 5 to 30 seconds.

   For example, the following command line changes the polling interval from 5 to 20 seconds:

   ```
   dlcmi/1/2# polling-interval 20
   dlcmi/1/2#
   ```

Full Enquiry Interval

To set the full enquiry interval:

1. **Navigate to the dlcmi prompt.**

   For example:

   ```
   box; frame-relay/1/2; dlcmi
   ```

2. **Enter the full-enquiry-interval command and the value you want the network to use.**

   full-enquiry-interval *<integer>*

   <integer> is the number of polling intervals that occur before the router sends a full status inquiry; the legal values are 1 to 255 intervals, and the default is 6.

   For example, the following command line sets the full enquiry interval to 45 seconds:

   ```
   dlcmi/1/2# full-enquiry-interval 45
   dlcmi/1/2#
   ```

Error Threshold

To set an error threshold:

1. **Navigate to the dlcmi prompt.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2; dlcmi
   ```

2. **Enter the error-threshold command and the value you want the network to use.**

   error-threshold *<integer>*

   <integer> is the number of status exchange errors that can occur during the number of monitored events you specify before the router brings down the connection. Legal values are 1 to 5000, and the default is 3.

   For example, the following command line sets the error threshold at 12 errors:

   ```
   dlcmi/1/2# error-threshold 12
   dlcmi/1/2#
   ```

Monitored Events

To set monitored events:

1. **Navigate to the dlcmi prompt.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2; dlcmi
   ```

2. **Enter the monitored-events command and the value you want the network to use.**

   monitored-events *<integer>*

   <integer> is the number of monitored events that together with the error threshold establishes a criterion to evaluate the quality of the router/frame relay connection. The legal values are 1 to 5000 events, and the default is 4.

   For example, the following command line sets the value at 10 events:

   ```
   dlcmi/1/2# monitored-events 10
   dlcmi/1/2#
   ```

Using Site Manager

To specify error threshold and monitored events values:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Interfaces**.	The Frame Relay Interfaces window opens.
4. Set the following parameters, using **Help** or the parameter descriptions that begin on page A-7: • **Polling Interval** • **Full Enquiry Interval** • **Error Threshold** • **Monitored Events**	

Site Manager Procedure *(continued)*	
You do this	**System responds**
5. Edit other parameters if you want, and click on **Apply**.	
6. Click on **Done**.	You return to the main Configuration Manager window.

Setting XOFF Control

You configure the router to ignore or observe the XOFF bit in LMI by using the BCC to set the XOFF control. The default is enabled.

To set the XOFF control:

1. **Navigate to the dlcmi prompt.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2; dlcmi
   ```

2. **Enter the xoff-control command and the value you want the network to use.**

   xoff-control *<value>*

   <value> can be **enabled** for the router to observe the XOFF bit or **disabled** for the router to ignore the XOFF bit.

   For example, the following command line disables XOFF control:

   ```
   dlcmi/1/2# xoff-control disabled
   dlcmi/1/2#
   ```

Customizing PVCs

Use the sections that follow for guidance in customizing PVCs to meet the requirements of your network.

You can use either the BCC or Site Manager to add service records for PVCs.

Adding Service Records for PVCs

A *service record* is a data structure that allows flexible grouping and characterization of PVCs. You can add and delete service records from your frame relay interfaces. When you add a new service record, it automatically creates one PVC to which you must assign a DLCI number.

Using the BCC

1. **Navigate to the frame-relay prompt.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2
   ```

2. **Enter the service command and a service name in this format:**

   service *<servicename>*

   For example, the following command line creates a service record with the name of "boston":

   ```
   frame-relay/1/2# service boston
   service/boston#
   ```

Using Site Manager

To add a service record:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on **Add**.	The Frame Relay Service Add window opens.
5. Click on the **DLCI Number** parameter, and enter the DLCI number. Note that the **Service Name** parameter is already filled in. See pages A-25 and A-24 for descriptions of these parameters.	

Site Manager Procedure *(continued)*	
You do this	**System responds**
6. Click on **OK.**	The Frame Relay Service List window reopens.
7. Add more service records as your network requires by repeating steps 4 through 6. When you are finished, click on **Done.**	The Frame Relay Circuit Definition window opens.
8. Click on **Done** again**.**	You return to the Configuration Manager window.

Deleting Service Records for PVCs

You can use either the BCC or Site Manager to delete service records for PVCs.

Using the BCC

1. **Navigate to the frame-relay prompt.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2
   ```

2. **Enter the delete command and the service command and name in this format:**

   delete service/*<servicename>*

   For example, the following command line deletes a service record with the name of “dallas”:

   ```
   frame-relay/1/2# delete service/dallas
   frame-relay/1/2#
   ```

Using Site Manager

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on the service record entry.	
5. Click on **Delete**.	Site Manager removes the service record entry from the Frame Relay Service List window.

Adding PVCs to Service Records

You can use either the BCC or Site Manager to add PVCs to already existing service records.

Using the BCC

You can add one or more PVCs at a time. To add one PVC:

1. **Navigate to the service record to which you want to add PVCs.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2; service/boston
   ```

2. **Enter the pvc command and a DLCI number in this format:**

   pvc <DLCI number>

   For example, the following command line creates a PVC with a DLCI of 20:

   ```
   service/boston# pvc 20
   pvc/3/2/20#
   ```

To add more than one PVC:

1. **Navigate to the service record to which you want to add PVCs.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2; service/4.0.32
   ```

2. **Enter the pvc command and DLCI number in this format:**

   pvc *<DLCI number>*; **pvc** *<DLCI number>*; **pvc** *<DLCI number>*; ...

   For example, the following command line creates PVCs with DLCI numbers 20, 21, 22, 23, and 24:

   ```
   service/boston# pvc 20; pvc 21; pvc 22; pvc 23; pvc 24;
   pvc/3/2/24#
   ```

   Note that the working context is now that of the PVC you made last.

Using Site Manager

You can add PVCs either individually, or in a range. If you want to add one PVC, enter one DLCI number. If you want to add several PVCs, enter the appropriate range of DLCI numbers in the format < *lowest DLCI number*> - < *highest DLCI number*>. To add PVCs:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on **PVCs**.	The Frame Relay PVC List window opens.
5. Click on **Add**.	The Frame Relay PVC Add window opens.

Site Manager Procedure *(continued)*	
You do this	**System responds**
6. Click on the **DLCI Number** parameter and enter the DLCI number, or, if you want to add more than one PVC, enter a range of numbers in the format *<lowest DLCI number> - <highest DLCI number>.*	
7. Click on **OK**.	The Frame Relay PVC List window reopens. Note that it now lists the PVCs you have just created.

Deleting PVCs from Service Records

You can delete PVCs from already existing service records. After you delete a PVC, it may reappear on the list of active PVCs if the switch provider does not delete it. As soon as the switch provider removes the PVC, frame relay dynamically deletes the PVC from the list.

If the switch provider deletes a PVC that you manually configured, the circuit state is set to invalid, and the PVC remains unused until you delete it from the interface.

You can use either the BCC or Site Manager to delete PVCs from service records.

Using the BCC

1. **Navigate to the frame-relay prompt.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2; service/dallas
   ```

2. **Enter the delete command and identify the PVC or PVCs you want to delete using this syntax:**

   delete pvc/*<port number>*/*<slot number>*/*<DLCI number>*;

   For example, the following command line deletes PVCs 51 and 52:

   ```
   service/dallas# delete pvc/1/2/51; delete pvc/1/2/52
   service/dallas#
   ```

Using Site Manager

To delete PVCs:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on **PVCs**.	The Frame Relay PVC List window opens.
5. Click on the PVC entry.	
6. Click on **Delete**.	The confirmation window closes. Site Manager removes the PVC entry from the Frame Relay PVC List window.

Moving PVCs from One Service Record to Another

You can use Site Manager to move PVCs on the same line from one service record to another. You can move PVCs to already existing or to new service records.

To move PVCs:

Site Manager Procedure	
You do this	**System responds**
1. Click on a port in the Configuration Manager window configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on **PVCs**.	The FR PVC List for Service window opens.

Site Manager Procedure *(continued)*	
You do this	**System responds**
5. Select the DLCI of the PVC to be moved, and click on **Move**.	The Frame Relay PVC Move window opens.
6. Click on **OK**.	The FR Service Record Selection window opens.
7. Click on the target service record and click on **Select**.	The FR Service Record Selection window closes, revealing the change in the FR PVC List for Service window.

Enabling Multicast

The multicast feature sets up a separate DLCI that replicates broadcast packets and forwards them to the appropriate destinations. You can enable support for frame relay multicast service, but only if your frame relay subscription service provides multicast service.

You can use either the BCC or Site Manager to enable multicast service.

Using the BCC

To enable multicast service, you must set the appropriate attribute for both the interface and the PVC:

1. **Navigate to the frame-relay prompt.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2
   ```

2. **Enter the multicast-control command and the value *enabled*:**

   multicast-control enabled

   For example, the following command line enables multicast for this frame relay interface:

   ```
   frame-relay/1/2# multicast-control enabled
   frame-relay/1/2#
   ```

3. **Navigate to the prompt for the PVC that you want to configure as multicast.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2; service/4.0.32; pvc/1/2/51
   ```

4. **Enter the multicast-control command and the value *enabled*:**

   multicast-control enabled

   For example, the following command line enables multicast for this PVC:

```
pvc/1/2/51# multicast-control enabled
pvc/1/2/51#
```

Using Site Manager

To enable multicast service, you must set the appropriate parameter for both the interface and the PVC:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Interfaces**.	The Frame Relay Interfaces window opens.
4. Set the **Multicast** parameter to **Enable**. See **Help** or the parameter description on page A-9.	
5. Edit other parameters if you want, and click on **Apply**.	
6. Click on **Done**.	You return to the main Configuration Manager window.
7. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
8. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
9. Click on **Services**.	The Frame Relay Service List window opens.
10. Click on **PVCs**.	The FR PVC List for Service window opens.
11. Set the **Multicast** parameter to **Multicast**. See **Help** or the parameter description on page A-27.	

Site Manager Procedure *(continued)*	
You do this	**System responds**
12. Edit other parameters if you want, and click on **Apply**.	
13. Click on **Done**.	You return to the main Configuration Manager window.

Configuring Hybrid Mode for PVCs

Hybrid mode allows you to use the same PVCs for both routing and bridging. You configure hybrid mode using Site Manager to set the Hybrid Mode parameter to ON.

To configure hybrid mode:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on **PVCs**.	The FR PVC List for Service window opens.
5. Set the **Hybrid Mode** parameter to **ON**. See **Help** or the parameter description on page A-28.	
6. Edit other parameters if you want, and click on **Apply**.	
7. Click on **Done**.	You return to the main Configuration Manager window.

Configuring PVC Pass-Through

To configure PVC pass-through service you create a mapping between PVCs on different lines. You can use a PVC for only one pass-through mapping.

To configure PVC pass-through:

Site Manager Procedure	
You do this	**System responds**
1. Configure at least two PVCs, using the directions in the previous sections. Remember that to use PVC pass-through you must configure the PVCs you want to map to each other on different lines.	
2. Set the **Hybrid Mode** parameter to **ON** for each of the PVCs that you want to configure for pass-through, following the procedure in the previous section.	
3. Edit other parameters if you want, and click on **Apply**.	The Select Protocols window opens.
4. Choose **FR PVC Passthru** from the menu options. You can also choose **WCP**, but configuring any other bridging protocols will have no effect.	
5. When you are finished, click on **OK**.	You return to the FR PVC List for Service window.
6. When you have finished adding PVCs, click on **Done**.	You return to the FR Service List window.
7. Click on **Done**.	You return to
8. Click on **Done**.	You return to the main Configuration Manager window.
9. Choose **Protocols** > **FR PVC Passthru** > **Mappings** from the menu bar.	The FR Passthru Mapping List window opens.
10. Choose **Add**.	The FR PVC Passthru Mapping Add window opens. It directs you to “Select first PVC for Passthru mapping:”
11. Choose the first PVC and click on **Select.**	The FR PVC Passthru Mapping Add window now displays a list of PVCs that you can map to the first PVC. This list consists of all PVCs that you have not already configured for a mapping, and that reside on lines other than the one for the first PVC. The window now instructs you to “Select second PVC for Passthru mapping:”

Site Manager Procedure *(continued)*	
You do this	**System responds**
12. Choose the PVC with which you want to map the PVC you chose in Step 9.	
13. Click on **Select**.	The FR Passthru Mapping List window now displays the mapping you just created.
14. Continue creating mappings. When you are finished, click on **Done**.	You return to the main Configuration Manager window.

Controlling Congestion for PVCs

Congestion occurs when a node receives more frames than it can process, or sends more frames than the transmission line can transport. You can enable congestion control on your network. When you enable congestion control, the router receives congestion notification messages from the PVC experiencing congestion, and drops all outbound traffic destined for that PVC until it no longer receives congestion notifications.

When you enable congestion control, you can set the length of time during which the router counts congestion notifications. You can also set the maximum number of congestion notifications that the router can receive during this time period. If the router receives this number of congestion notifications within the time period you specify, it stops transmitting data. The router resumes transmission when it stops receiving congestion notifications.

If you use traffic shaping with congestion control, you also need to decide which congestion control method you want the router to use. For more information about traffic shaping, see “Using Traffic Shaping With PVCs” on page 3-29.

You can use either the BCC or Site Manager to control congestion for PVCs.

Using the BCC

If you enable congestion control, all PVCs on the interface use congestion control and the values you specify for the congestion timer and congestion counter, unless you configure PVCs individually at the service level and either disable congestion control or select other values for the congestion control attributes.

Configuring Congestion Control for an Interface

To configure congestion control for the interface you must first enable congestion control, then optionally you can set a value for the congestion timer, congestion counter, and the congestion method.

Congestion Control

1. **Navigate to the frame-relay prompt.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2
   ```

2. **Enter the congestion-control command and the value *enabled*:**

   congestion-control enabled

   For example, the following command line enables congestion control for this frame relay interface:

   ```
   frame-relay/1/2# congestion-control enabled
   frame-relay/1/2#
   ```

Congestion Timer

To change the value for the congestion timer:

1. **Navigate to the prompt for the interface that you want to edit.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2
   ```

2. **Enter the congestion-timer command and the value you want the interface to use:**

   congestion-timer *<integer>*

   <integer> is the length of time, in seconds, during which the router counts congestion notifications (see "Congestion Counter" on page 3-24). If the router receives the number of congestion notifications you set in the Congestion Counter during this amount of time, the router stops transmitting data.

   Legal timer values are 0.5, 1, 1.5, 2, 2.5, 3, 3.5, 4, 4.5, and 5 seconds. The default is 1 second.

For example, the following command line sets a congestion timer of 2.5 seconds:

```
frame-relay/1/2# congestion-timer 2.5
frame-relay/1/2#
```

Congestion Counter

To change the value for the congestion counter:

1. **Navigate to the prompt for the interface that you want to edit.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2
   ```

2. **Enter the congestion-counter command and the value you want the interface to use:**

   congestion-counter *<integer>*

   <integer> is the maximum number of congestion notifications the router can receive during the Congestion Timer period before it stops transmitting data.

   Legal counter values are 1 to 500 notifications. The default is 20.

   For example, the following command line sets a congestion counter of 30 notifications:

   ```
   frame-relay/1/2# congestion-counter 30
   frame-relay/1/2#
   ```

Congestion Method

To change the value for the congestion method:

1. **Navigate to the prompt for the interface that you want to edit.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2
   ```

2. **Enter the congestion-method command and the value you want the interface to use:**

   congestion-method *<value>*

   Legal values are:

   throttle-then-shutdown
   shutdown (the default)
   throttle

   For example, the following command line sets a congestion method of throttle:

   ```
   frame-relay/1/2# congestion-method throttle
   frame-relay/1/2#
   ```

Configuring Congestion Control for Individual PVCs

To enable or change congestion control for a PVC:

Congestion Control

1. **Navigate to the prompt for the PVC you want to edit.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2;dallas; pvc/1/2/51;
   ```

2. **Enter the congestion-control command and the value you want the interface to use:**

   congestion-control *<value>*

   Legal values are:

   enabled
   disabled
   inherit

For example, the following command line enables congestion control for this frame relay interface:

```
pvc/1/2/51# congestion-control enabled
pvc/1/2/51#
```

Congestion Timer

To change the value for the congestion timer:

1. **Navigate to the prompt for the PVC that you want to edit.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2; dallas; pvc/1/2/51
   ```

2. **Enter the congestion-timer command and the value you want the interface to use:**

   congestion-timer *<integer>*

   <integer> is the length of time, in seconds, during which the router counts congestion notifications (see "Congestion Counter" on page 3-26, following). If the router receives the number of congestion notifications you set in the congestion counter during this amount of time, the router stops transmitting data.

   Legal timer values are 0.5, 1, 1.5, 2, 2.5, 3, 3.5, 4, 4.5, and 5 seconds. The default is 1 second.

   For example, the following command line sets a congestion timer of 2.5 seconds:

   ```
   pvc/1/2/51# congestion-timer 2.5
   pvc/1/2/51#
   ```

Congestion Counter

To change the value for the congestion counter:

1. **Navigate to the prompt for the PVC that you want to edit.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2; orlando; pvc/1/2/51
   ```

2. **Enter the congestion-counter command and the value you want the interface to use:**

   congestion-counter *<integer>*

   <integer> is the maximum number of congestion notifications the router can receive during the congestion timer period before it stops transmitting data.

   Legal counter values are 1 to 500 notifications. The default is 20.

   For example, the following command line sets a congestion counter of 30 notifications:

```
pvc/1/2/51## congestion-counter 30
pvc/1/2/51##
```

Congestion Method

To change the value for the congestion method:

1. **Navigate to the prompt for the PVC that you want to edit.**

   For example:

```
box; serial/1/2; frame-relay/1/2; newyork; pvc/1/2/51
```

2. **Enter the congestion-method command and the value you want the interface to use:**

   congestion-method *<value>*

   Legal values are:

   throttle-then-shutdown
   shutdown (the default)
   throttle
   inherit

   For example, the following command line sets a congestion method of throttle:

```
pvc/1/2/51# congestion-method throttle
pvc/1/2/51#
```

Using Site Manager

You can enable congestion control for the interface, and you can also customize values for individual PVCs.

To enable congestion control for the interface:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Interfaces**.	The Frame Relay Interfaces window opens.
4. Set the following parameters, using **Help** or the parameter descriptions that begin on page A-9: • **Congestion Control** • **Congestion Timer** • **Congestion Counter** • **Congestion Method** (applies only when you enable traffic shaping)	
5. Edit other parameters if you want, and click on **Apply**.	
6. Click on **Done**.	You return to the main Configuration Manager window.

To customize congestion control for individual PVCs:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Services**.	The Frame Relay Service List window opens.

Site Manager Procedure *(continued)*	
4. Click on **PVCs**.	The FR PVC List for Service window opens.
5. Set the following parameters, using **Help** or the parameter descriptions that begin on page A-29: • **Congestion Control** • **Congestion Timer** • **Congestion Counter** • **Congestion Method** (applies only when you enable traffic shaping)	
6. Edit other parameters if you want, and click on **Apply**.	
7. Click on **Done**.	You return to the main Configuration Manager window.

Using Traffic Shaping With PVCs

Traffic shaping relieves bottlenecks in networks. To enhance the effectiveness of traffic shaping, you may also want to edit values for the PVC Congestion Control and Congestion Method attributes or parameters. For more information about the interaction between these attributes or parameters, and traffic shaping see “Traffic Shaping Considerations,” on page 2-29.

You can use either the BCC or Site Manager to configure traffic shaping.

Using the BCC

To enable traffic shaping, you configure values for High Queue Limit, Low Queue Limit, Committed Burst, Excess Burst, and Throughput.

High Queue Limit

The high queue limit specifies the maximum number of buffers queued in high queue for PVC. To change the high queue limit:

high-queue-limit *<integer>*

Low Queue LImit

The low queue limit specifies the maximum number of buffers queued in low queue for PVC. To change the low queue limit:

high-queue-limit *<integer>*

Committed Burst

The committed burst rate (B_c) defines the number of bits the router can transmit over a specified time interval when congestion occurs. Set this attribute to 1/4 the value of the CIR unless this VC is sending frames larger than that size, in which case you should increase the value the committed burst to accommodate that frame size.

To change the value for the committed burst:

1. **Navigate to the prompt for the PVC that you want to edit.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2; orlando; pvc/1/2/51
   ```

2. **Enter the committed-burst command and the value you want the PVC to use:**

   committed-burst *<integer>*

   <integer> is the number of bits the router can transmit per time interval.

   Legal values are 0 to 2,147,483,647 bits. The default is 0.

   For example, the following command line sets a committed burst value of 4,000 bits.

   ```
   pvc/1/2/51# committed-burst 4000
   pvc/1/2/51#
   ```

Excess Burst

The excess burst rate (B_e) combines with the committed burst rate to determine the maximum number of bits the router can transmit over a specified time interval when there is no congestion. The excess burst plus the committed burst must be less than or equal to the line speed. To change the value for the excess burst:

1. **Navigate to the prompt for the PVC that you want to edit.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2; orlando; pvc/1/2/51
   ```

2. **Enter the excess-burst command and the value you want the PVC to use:**

   excess-burst *<integer>*

   <integer> is the number of bits the router can transmit per time interval.

   Legal values are 0 to 2,147,483,647 bits. The default is 0.

   For example, the following command line sets an excess burst value of 2,000 bits:

   ```
   pvc/1/2/51# committed-burst 2000
   pvc/1/2/51#
   ```

CIR (Throughput)

The CIR (committed information rate) defines the number of bits per second your carrier guarantees the router can transmit over a specified time interval when there is no congestion. Your carrier supplies this value:

1. **Navigate to the prompt for the PVC that you want to edit.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2; newyork; pvc/1/2/51
   ```

2. **Enter the** cir **command and the value you want the PVC to use:**

   cir *<integer>*

   <integer> is the number of bits the router can transmit per time interval.

   Legal values are 0 to 2,147,483,647 bits. The default is 0.

For example, the following command line sets a CIR value of 5,000 bits.

```
pvc/1/2/51# committed-burst 5000
pvc/1/2/51#
```

Using Site Manager

To enable traffic shaping:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Select the appropriate service record and click on **PVCs**.	The Frame Relay PVC List window opens.
5. Click on a PVC that you want to configure for traffic shaping.	
6. Configure the following traffic shaping parameters, using **Help** or the parameter descriptions that begin on page A-28: • **Committed Burst** • **Excess Burst** • **Throughput**	The parameters are now set to the values you chose.
7. Click on **Done**.	You return to the Frame Relay Service List window.
8. Click on **Done**.	You return to the Frame Relay Circuit Definition window.
9. Click on **Done**.	You return to the main Configuration Manager window.

Enabling Compression for PVCs

To use data compression with frame relay, first select WCP from the Protocols menu, and make sure the Compression Control attribute or parameter is set to Enable. You can use either the BCC or Site Manager to enable compression for PVCs.

Using the BCC

The default value for the **wcp-control** command is *enabled*. To disable compression for this virtual circuit:

1. **Navigate to the prompt for the PVC that you want to edit.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2; boston; pvc/1/2/51
   ```

2. **Enter the wcp-control command and the value *disabled*:**

   wcp-control disabled

   For example, the following command line disable compression for this virtual circuit:

   ```
   pvc/1/2/51# wcp-control disabled
   pvc/1/2/51#
   ```

Using Site Manager

To enable data compression:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on **PVCs**.	The FR PVC List for Service window opens.
5. Set the **Compression Control** parameter to **Enable**. See **Help** or the parameter description on page A-31.	
6. Edit other parameters if you want, and click on **Apply**.	
7. Click on **Done**.	You return to the main Configuration Manager window.

Grouping Service Records for Multiline Mode

Using Site Manager, you can configure two or more service records to run in multiline mode (for information about Bay Networks proprietary implementation of multiline, see page 2-35.) Service records that you group for multiline must:

- Reside on two separate physical ports
- Have the same DLCI numbers
- Not use hybrid mode

To configure multiline mode:

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on the **Multiline** button.	The Services Multiline With window opens.
5. Click on the **Add** button.	The Add Multiline Services window opens.
6. Choose the frame relay interface you want to configure for multiline.	The frame relay interface entry becomes highlighted.
7. Click on **Select**.	The Add Multiline Services window closes. Site Manager moves the record of the frame relay interface from the Add Multiline Services window to the Services Multiline With window.
8. Set the **Multiline Algorithm to Choose Line** parameter. Use **Help** or see the parameter description on page A-34.	
9. Click on **Apply**.	
10. Click on **Done**.	You return to the Frame Relay Service List window.

Removing Multiline Services

To remove multiline services:

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on the **Multiline** button.	The Services Multiline With window opens.
5. Choose the frame relay interface you want to remove in the Services Multiline With window.	The frame relay interface becomes highlighted.
6. Click on the **Remove** button.	Site Manager removes the record of the frame relay interface from the Services Multiline With window.

For information about the Bay Networks proprietary implementation of multiline, see page 2-35.

Customizing SVCs

Use the sections that follow for guidance on customizing SVCs to meet the requirements of your network.

Adding Service Records for SVCs

A *service record* is a data structure that allows flexible grouping and characterization of VCs. To configure service records for SVCs, you:

- Provide a name for the service record.
- Enable SVC services.
- Provide an address for the SVC.

You can also:

- Enable call screening and blocking.
- Customize the inactivity timer and mode.

You can use either the BCC or Site Manager to configure service records for SVCs.

Using the BCC

To use the BCC to configure SVCs:

1. **Navigate to the frame-relay prompt.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2
   ```

2. **Enter the service command and a service name in this format:**

   service *<servicename> <line number>*.0.*<circuit number>*

   For example, the following command line creates the service record 8.0.32:

   ```
   frame-relay/1/2# service myservice 8.0.32
   myservice/8.0.32#
   ```

3. **Enter the svc-control command and the value *enabled*.**

   svc-control enabled

   For example, the following command line enables SVCs on this service record:

   ```
   myservice/8.0.32#  svc-control enabled
   myservice/8.0.32#
   ```

4. **Enter the svc-local-address command and the address.**

   For example, the following specify a local address in X.121 or E.164 format:

   ```
   myservice/8.0.32#  svc-local-address e164, 1234567, 1234567,
   International
   myservice/8.0.32#  svc-local-address e164, 1234567, 1234567, Unknown
   myservice/8.0.32#  svc-local-address x121, 1234567, 1234567,
   International
   myservice/8.0.32#  svc-local-address e164, 1234567, 1234567, Unknown
   myservice/8.0.32#
   ```

Using Site Manager

To add service records to a frame relay interface:

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on **Add.**	The Frame Relay Service Add window opens.
5. Set the **SVC Support** parameter to **Enable**. Use **Help** or the parameter description on page A-36.	The SVC parameters become available.
6. Set the following SVC parameters. Use **Help** or the parameter descriptions that begin on page A-36: • **SVC Local Party Number** • **SVC Local Party SubAddress** (optional) • **SVC Local Party Number Plan** • **SVC Local Party Type of Number**	
7. Click on **Apply**.	The SVC button replaces the Multiline button in the Frame Relay Service List window.
8. Click on **Done**.	

Deleting Service Records for SVCs

You can use either the BCC or Site Manager to delete service records for SVCs.

Using the BCC

To delete service records:

1. **Navigate to the frame-relay prompt.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2
   ```

2. **Enter the delete command and the service command and name in this format:**

   delete service/*<servicename>*

   For example, the following command line deletes the service record 8.0.32:

```
frame-relay/1/2# delete service/8.0.32
frame-relay/1/2#
```

Using Site Manager

To delete service records from a frame relay interface:

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Choose the service record you want to delete.	
5. Click on **Delete**.	A confirmation window opens. It asks if you really want to delete the service record.
6. Click on **OK.**	You have deleted the service record.

Call Screening and Blocking

You can use either the BCC or Site Manager to configure call screening and blocking for a service record.

Using the BCC

You can screen and block incoming calls. The relevant commands are:

- **svs-call-block-direction**
- **svc-screen-control**
- **svc-screen-usage**

SVC Call Block Direction

The **svc-call-block-direction** command enables you to block certain type of calls on the SVC. Legal values are:

both
none
inbound
outbound
all

To set SVC call block direction:

1. **Navigate to the service prompt.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2; service/8.0.32
   ```

2. **Enter the svc-call-block-direction command, and one of these options:**

   For example, the following command line sets a call block direction of outbound:

   ```
   service/8.0.32#  svc-call-block-direction outbound
   service/8.0.32
   ```

SVC Screening

The **svc-screen-control** command enables you screen incoming calls on this service record. Legal values are enabled and disabled. The default is disabled.

To set SVC screen usage:

1. **Navigate to the service prompt.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2; service/8.0.32
   ```

2. **Enter the svc-screen-control command, and set it to *enabled*.**

   For example, the following command line enables call screening:

   ```
   service/8.0.32#  svc-screen-control enabled
   service/8.0.32
   ```

SVC Screen Usage

The **svc-screen-usage** command enables you to allow or disallow calls from numbers in associated SVC option records. Legal values are **include** which allows these calls, and **exclude**, which disallows them. The default is include.

To set SVC screen usage:

1. **Navigate to the service prompt.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2; service/8.0.32
   ```

2. **Enter the svc-screen-usage command, and set it to *include* or *exclude*.**

   For example, the following command line disallows calls from numbers in associated SVC option records:

   ```
   service/8.0.32#  svc-screen-usage exclude
   service/8.0.32#
   ```

Using Site Manager

To configure call block and screening for a frame relay service record:

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Set the following parameters, using **Help** or the parameter descriptions that begin on page A-38: • **SVC Call Block** • **SVC InScreening Disable** • **SVC InScreening Usage**	
5. Click on **Apply**.	
6. Click on **Done**.	

Adding SVC Options to Service Records

You can use either the BCC or Site Manager to add SVC options to service records.

Using the BCC

To add SVC options:

1. **Navigate to the service record to which you want to add SVCs.**

   For example:

   ```
   box; serial/3/2; frame-relay/3/2; service/8.0.32
   ```

2. **Enter the svc-options command and a name for the SVC in the format:**

   svc-options *<name>*

   For example, the following command line adds the SVC Toronto:

   ```
   service/8.0.32# svc-options Toronto
   service/8.0.32#
   ```

Using Site Manager

To add SVCs to already existing service records:

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Choose the service records to which you want to add SVCs, and set the **SVC Support** parameter to **Enable**. Use **Help** or the parameter description on page A-36.	The SVC parameters become available.

Site Manager Procedure *(continued)*	
You do this	**System responds**
5. Supply values for the following SVC parameters. Use **Help** or the parameter descriptions that begin on page A-36. • **SVC Local Party Number** • **SVC Local Party Sub-Address (optional)** • **SVC Local Party Number Plan** • **SVC Local Party Type of Number**	
6. Click on **Apply**.	The SVC button replaces the Multiline button in the Frame Service List window
7. Click on the **SVC** button.	The Frame Relay Options List for Service window opens.
8. Click on **Add**.	The Frame Relay SVC Options Add window opens.
9. Supply values for the following SVC parameters. Use **Help** or the parameter descriptions in Appendix A. • **Remote Party Number** • **Remote Party Sub-Address**	
10. When you are finished, click on **OK**.	You return to the Frame Relay Options List for Service window.
11. Add as many SVC options as your network requires. When you are finished, click on **Done**.	You return to the Frame Relay Service List window.
12. Click on **Done**.	You return to the main Configuration Manager window.

Disabling SVCs

You can use either the BCC or Site Manager to disable SVC options without deleting them.

Using the BCC

To disable SVCs:

1. **Navigate to the SVC options you want to disable.**

For example:

```
box; serial/3/2; frame-relay/3/2; service/8.0.3; svc-options/toronto
```

2. **Enter the state command and the *disabled* option.**

   For example, the following command line disables the SVC toronto:

```
svc-options/toronto# state disabled
svc-options/toronto#
```

Using Site Manager

To disable SVCs:

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Choose the service record that includes the SVCs you want to disable.	
5. Choose the SVC you want to delete.	
6. Set the **SVC Support** parameter to **Disable**.	You have disabled the SVC.
7. Click on **Apply**.	The Multiline button replaces the SVC button in the Frame Relay Service List window.
8. Click on **Done**	You return to the main Configuration Manager window.

Disconnecting Active SVCs

To disconnect an active SVC:

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Choose the service record that includes the SVCs you want to disconnect.	
5. Click on the **SVCs** button	The Frame Relay SVC Options List for Service window opens.
6. Click on the **Active Calls** button	The Frame Relay SVC Active Calls window opens.
7. Choose the **DLCI** of the SVC you want to disconnect.	
8. Click on **Delete**.	The SVC Active Call Delete Query window opens.
9. Click on **Yes**.	You have disconnected the SVC. You return to the Frame Relay SVC Active Calls window.
10. Click on **Done**.	You return to the Frame Relay SVC Options List for Service window.
11. Click on **Done**.	You return to the Frame Relay Service List window.
12. Click on **Done**.	You return to the Main Configuration Manager window.

Editing LAPF Parameters for SVCs

Frame relay LAPF services support the reliable transfer of multiple numbered frames over SVCs. You can use either the BCC or Site Manager to customize LAPF.

Using the BCC

You can edit the following parameters for LAPF in the BCC, as described in this section:

- State
- Station Type
- Initiation Mode
- Retransmission Timer
- Idle Timer
- Retransmission Limit
- Information Limit
- Window Size

State

State controls whether LAPF is enabled or disabled. To change this value:

1. **Navigate to the LAPF prompt.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2; lapf/1/2
   ```

2. **Enter the state command and the value you want to use.**

   state *<value>*

   Values are **enabled** and **disabled**. The default is **enabled**.

   For example, the following command line disables LAPF.

   ```
   lapf/3/2# state disabled
   lapf/3/2#
   ```

Station Type

Station Type determines whether the interface acts as the DCE or DTE. To change this value:

1. **Navigate to the LAPF prompt.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2; lapf/1/2
   ```

2. **Enter the station-type command and one of the following options:**

   dce
   dte
   networkside (which means DCE)
   userside (which means DTE)

   For example, the following command line sets station type DCE:

```
lapf/3/2# station-type dce
lapf/3/2#
```

Initiation Mode

Initiation mode determines the action LAPF will take to initiate link setup by sending or holding unnumbered command (SABME) frames to poll the router at the other end of the connection. To set the initiation mode:

1. **Navigate to the LAPF prompt.**

   For example:

```
box; serial/1/2; frame-relay/1/2; lapf/1/2
```

2. **Enter the initiation-mode command and either *active* (the default) or *passive*.**

   Active indicates that LAPF will send SABME frames and initiate link setup. Passive indicates that LAPF takes no action to initiate link setup. The default is active.

   For example, the following command line sets an initiation mode of passive:

```
lapf/3/2# initiation-mode passive
lapf/3/2#
```

Retransmission Timer

Retransmission timer is the general purpose retransmission timeout. It is used during initiation of LAPF multiple frame support, and for timeout of LAPF numbered information frames. In the event of a timeout, the sending platform retransmits the frame, up to the maximum number of times you specify for **retransmission limit.** To set the retransmission timer:

1. **Navigate to the LAPF prompt.**

   For example:

```
box; serial/1/2; frame-relay/1/2; lapf/1/2
```

2. **Enter the retransmission-timer command and the value you want to use.**

   retransmission-timer *<integer>*

   <integer> is the length of time that the router waits to receive an acknowledgment. Legal values are 1 to 1200 tenths of a second. The default is 15.

   For example, the following command line sets a timer of 30 tenths of a second (3 seconds):

```
lapf/3/2# retransmission-timer 30
lapf/3/2#
```

Idle Timer

Idle timer indicates the amount of time that the router allows with no data being transmitted. In the event of a timeout, the router initiates a frame handshake to check if the connection is still up. To set the idle timer:

1. **Navigate to the LAPF prompt.**

   For example:

```
box; serial/1/2; frame-relay/1/2; lapf/1/2
```

2. **Enter the** idle-timer **command and the value you want to use.**

   idle-timer *<integer>*

   <integer> is the length of time that the router allows with no data being transmitted. Legal values are 1 to 120 seconds. The default is 30.

   For example, the following command line sets a timer of 18 seconds:

```
lapf/3/2# idle-timer 18
lapf/3/2#
```

Retransmission Limit

Retransmission limit indicates the maximum number of LAPF retransmissions that can occur after the retransmission timer expires. The connection terminates if the router reaches the retransmission limit. To set the retransmission limit:

1. **Navigate to the LAPF prompt.**

   For example:

```
box; serial/1/2; frame-relay/1/2; lapf/1/2
```

2. **Enter the retransmission-limit command and the value you want to use.**

   retransmission-limit *<integer>*

   <integer> is the number of times that the router retransmits after the retransmission timer expires. Legal values are 1 to 20. The default is 3.

   For example, the following command line sets a retransmission limit of 8 tries:

```
lapf/3/2# retransmission-limit 8
lapf/3/2#
```

Information Limit

Information limit indicates the maximum number octets of data allowed in the LAPF information field. The larger the number allowed, the less overhead on the system. However, a large value could exceed the system buffer size. You should accept the default value. To set the information limit:

1. **Navigate to the LAPF prompt.**

   For example:

```
box; serial/1/2; frame-relay/1/2; lapf/1/2
```

2. **Enter the information-limit command and the value you want to use.**

   information-limit *<integer>*

   <integer> is the number of octets. Legal values are 260 to 2052. The default is 260.

   For example, the following command line sets an information limit of 350:

```
lapf/3/2# information-limit 350
lapf/3/2#
```

Window Size

Window size indicates the maximum number of outstanding numbered information (I) frames allowed across a connection. These are frames that have travelled across the link, but which the peer has not acknowledged. Each of these frames remains in a backup queue until the peer sends an acknowledge message. A longer queue adversely affects performance. You should accept the default. To set the window size:

1. **Navigate to the LAPF prompt.**

For example:

```
box; serial/1/2; frame-relay/1/2; lapf/1/2
```

2. **Enter the window-size command and the value you want to use.**

   window-size *<integer>*

   <integer> is the number of outstanding frames allowed. Legal values are 1 to 127. The default is 7.

   For example, the following command line sets a window size of 45:

```
lapf/3/2# window-size 45
lapf/3/2#
```

Using Site Manager

To edit LAPF parameters:

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Interfaces**.	The Frame Relay Interface List window opens.
4. Click on the **LAPF** button.	The Frame Relay LAPF Parameters window opens.
5. Edit the following parameters. Use **Help** or the parameter descriptions in Appendix A as a guide. • **Enable** • **Station Type** • **Action Initiate** • **T200, Base Timer** • **T203, Idle Timer** • **N200 Max Retries** • **N201, Max Frame Size** • **K, Max Window Size**	
6. When you are finished, click on **OK**.	You return to the Frame Relay Interface List window.
7. Click on **Done**.	You return to the main Configuration Manager window.

Editing Signaling Attributes or Parameters for SVCs

A DTE and the frame relay network exchange various type of signaling messages, including incoming and outgoing call setup, call proceeding, connect and disconnect, and release messages. You can use either the BCC or Site Manager to customize signaling attributes or parameters.

Using the BCC

To edit signaling attributes:

State

State controls whether signaling is enabled or disabled. To change this value:

1. **Navigate to the signaling prompt.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2; signalling/1/2
   ```

2. **Enter the state command and the value you want to use.**

   state *<value>*

   Legal values are **enabled** and **disabled**. The default value is **enabled**.

   For example, the following command line disables signaling.

   ```
   signalling/3/2# state disabled
   signalling/3/2#
   ```

Maximum SVCs

Maximum SVCs indicates the maximum number of simultaneous switched virtual circuits allowed on the port. The more SVCs you allow, the larger the system memory required to support them. To set the window size:

1. **Navigate to the signaling prompt.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2; signalling/1/2
   ```

2. **Enter the maximum-svcs command and the value you want to use.**

   maximum-svcs *<integer>*

   <integer> is the number of SVCs allowed. Legal values are 1 to 2147483647. The default is 100.

For example, the following command line sets a maximum of 200 SVCs:

```
signalling/3/2# maximum-svcs 200
signalling/3/2#
```

Setup Timer

Setup timer indicates the number of seconds allowed from the time the router sends a setup message to the called subscriber and receives a connect or call proceeding message from the called subscriber. If a timeout occurs, the router retransmits the setup message and restarts the timer. If the timer expires a second time, the call is cleared. To set the setup timer:

1. **Navigate to the signaling prompt.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2; signalling/1/2
   ```

2. **Enter the setup-timer command and the value you want to use.**

   setup-timer *<integer>*

   <integer> is the number of seconds allowed. Legal values are 2 to 90 seconds. The default is 4.

   For example, the following command line sets a timer of 10 seconds:

   ```
   signalling/3/2# setup-timer 10
   signalling/3/2#
   ```

Disconnect Timer

Disconnect timer indicates the number of seconds allowed from the time the router sends a disconnect message and receives a release message back. If a timeout occurs, the router sends a release message and enters the release request state. The timer is not restarted. To set the disconnect timer:

1. **Navigate to the signaling prompt.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2; signalling/1/2
   ```

2. **Enter the disconnect-timer command and the value you want to use.**

   disconnect-timer *<integer>*

<integer> is the number of seconds allowed. Legal values are 20 to 90 seconds. The default is 30.

For example, the following command line sets a timer of 45 seconds:

```
signalling/3/2# disconnect-timer 45
signalling/3/2#
```

Release Timer

Release timer indicates the number of seconds allowed for call clearing initiated by the other end of the connection or when the disconnect timer expires. If a timeout occurs, the router retransmits the release message and restarts the timer. If the timer expires a second time, the call is cleared. To set the release timer:

1. **Navigate to the signaling prompt.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2; signalling/1/2
   ```

2. **Enter the release-timer command and the integer value you want to use.**

   release-timer *<integer>*

   <integer> is the number of seconds allowed. Legal values are 2 to 90 seconds. The default is 4.

   For example, the following command line sets a timer of 45 seconds:

   ```
   signalling/3/2# release-timer 45
   signalling/3/2#
   ```

Call Proceeding Timer

Call proceeding timer indicates the number of seconds allowed from the time the router receives a call proceeding message to the time the router receives a connect or disconnect message. In the event of a timeout, the router clears the call. To set the release timer:

1. **Navigate to the signaling prompt.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2; signalling/1/2
   ```

2. **Enter the call-proceeding-timer command and the integer value you want to use.**

   call-proceeding-timer *<integer>*

<integer> is the number of seconds allowed. Legal values are 2 to 90 seconds. The default is 10.

For example, the following command line sets a timer of 45 seconds:

```
signalling/3/2# call-proceeding-timer 45
signalling/3/2#
```

Status Enquiry Timer

Status enquiry timer indicates the number of seconds allowed from the time the router sends a status inquiry message to the time the router receives an incoming status, disconnect, release, or release complete message. If a timeout occurs, the router retransmits the status inquiry and restarts the timer. This occurs for the number of times set in the Status Enquiry Retry attribute, after which the call is cleared. To set the status enquiry timer:

1. **Navigate to the signaling prompt.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2; signalling/1/2
   ```

2. **Enter the status-enquiry-timer command and the integer value you want to use.**

   statis-enquiry-timer *<integer>*

   <integer> is the number of seconds allowed. Legal values are 2 to 90 seconds. The default is 4.

   For example, the following command line sets a timer of 30 seconds:

   ```
   signalling/3/2# status-enquiry-timer 30
   signalling/3/2#
   ```

Status Enquiry Retry

Status enquiry retry indicates the maximum number of times the router will retransmit a status inquiry message. If the router sends the maximum number of status inquiry messages and receives no response, the call is cleared. To set the status enquiry retry attribute:

1. **Navigate to the signaling prompt.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2; signalling/1/2
   ```

2. **Enter the status-enquiry-retry command and the integer value you want to use.**

   status-enquiry-retry *<integer>*

   <integer> is the number of retries. Legal values are 1 to 20 retries. The default is 4.

   For example, the following command line sets a value of 7 retries:

```
signalling/3/2# status-enquiry-retry 7
signalling/3/2#
```

Using Site Manager

To edit signaling parameters:

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Interfaces**.	The Frame Relay Interface List window opens.
4. Click on the **Signaling** button.	The Frame Relay Signaling Parameter window opens.
5. Edit the following parameters. Use **Help** or the parameters descriptions that begin on page A-18. • **Signaling Control** • **Max SVCs** • **T303, Setup Message Timer** • **T305, Disconnect Timer** • **T308, Release Timer** • **T310, Call Proceding Timer** • **T322, Status Enq Retry Timer** • **N322, Status Enq Retry Max**	
6. When you are finished, click on **OK**.	You return to the Frame Relay Interface List window.
7. Click on **Done**.	You return to the main Configuration Manager window.

Setting Inactivity Values for SVCs

The inactivity timer and inactivity mode timer attributes and parameters control how and when the router disconnects SVCs according to values that you configure for amount of time and the direction that data is flowing. You can set values for a service record, or for individual SVCs.

You can use either the BCC or Site Manager to set inactivity values for SVCs.

Using the BCC

You can use the BCC to set values for a service record or for individual SVCs.

Service Record Inactivity Values

To set inactivity values for a service record:

1. **Navigate to the service record.**

   For example:

   ```
   box; serial/3/2; frame-relay/3/2; service/8.0.32
   ```

2. **Enter the svc-inactivity-timer command with the integer value you want to use:**

   svc-inactivity-timer *<integer>*

   <integer> is the length of time, in seconds, before the SVC terminates because no data has travelled over the circuit in the direction you specify in the inactivity-direction attribute.

   Legal timer values are 0 to 2147483647 seconds. The default is 60 seconds.

   For example, the following command line sets the inactivity timer to 90 seconds:

   ```
   service/8.0.32# svc-inactivity-timer 90
   service/8.0.32#
   ```

3. **Enter the svc-inactivity-direction command with the value you want to use:**

   svc-inactivity-direction *<value>*

   Legal direction values are:

both
outbound
inbound
either

For example, the following command line sets the inactivity direction to outbound:

```
service/8.0.32# svc-inactivity-direction outbound
service/8.0.32#
```

Inactivity Values for an SVC

To set the inactivity timer and direction for a particular SVC option record:

1. **Navigate to the SVC options.**

   For example:

   ```
   box; serial/3/2; frame-relay/3/2; service/8.0.32; svc-options/toronto
   ```

2. **Enter the inactivity-timer command with the value you want to use:**

   inactivity-timer *<integer>*

   <integer> is the length of time, in seconds, before the SVC terminates because no data has travelled over the circuit in the direction you specify in the inactivity-direction attribute.

   Legal timer values are 0 to 2147483647 seconds. The default is 60 seconds.

   For example, the following command line sets the inactivity timer to 90 seconds:

   ```
   service/8.0.32# inactivity-timer 90
   service/8.0.32#
   ```

3. **Enter the inactivity-direction command with the value you want to use:**

   inactivity-direction *<value>*

   Legal direction values are:

   both
   outbound
   inbound
   either

   For example, the following command line sets the inactivity direction to outbound:

```
service/8.0.32# svc-inactivity-direction outbound
service/8.0.32#
```

Using Site Manager

To set inactivity values for a service record:

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Choose the service record for which you want to configure inactivity values.	
5. Set the following parameters, using **Help** or the parameter descriptions that begin on page A-44. • **Inactivity Timer** • **Inactivity Mode Timer**	
6. Click on **Apply**.	
7. Click on **Done**.	
8. Click on **Done.**	

To set the inactivity timer value and mode for a particular SVC:

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Choose the service record for which you want to configure inactivity values.	

Site Manager Procedure *(continued)*	
You do this	**System responds**
5. Click on SVCs.	The Frame Relay SVC Options List window opens.
6. Choose the SVC option record that has values in the following parameters that match the remote end of the SVC connection. • **Remote Party Number** • **Remote Party SubAddress (optional)** • **Remote Party Number Plan** • **Remote Party Type of Number**	
7. Set the following parameters, using **Help** or the parameter descriptions that begin on page A-44. • **Inactivity Timer** • **Inactivity Mode Timer**	
8. Click on **Apply**.	
9. Click on **Done**.	You return to the Frame Relay Service List window.
10. Click on **Done.**	You return to the main Configuration Manager window.

Controlling Congestion for SVCs

Congestion occurs when a node receives more frames than it can process, or sends more frames than the transmission line can transport. When you enable congestion control, the router receives congestion notification messages from the SVC experiencing congestion, and drops all outbound traffic destined for that SVC until it no longer receives congestion notifications.

When you enable congestion control, you can set the length of time during which the router counts congestion notifications. You can also set the maximum number of congestion notifications that the router can receive during this time period. If the router receives this number of congestion notifications within the time period you specify, it stops transmitting data. The router resumes transmission when it stops receiving congestion notifications.

If you enable congestion control, all SVCs on the interface use congestion control and the values you specify for the congestion timer and congestion counter, unless you configure SVCs individually and either disable this feature or select other values for the congestion control attributes and parameters.

You can use either the BCC or Site Manager to control congestion for SVCs.

Using the BCC

You can use the BCC to configure congestion control for an interface, or for individual SVCs.

Configuring Congestion Control for an Interface

You can edit the following attributes in the BCC:

- Congestion Control
- Congestion Timer
- Congestion Counter
- Congestion Method

Congestion Control

1. **Navigate to the frame-relay prompt.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2
   ```

2. **Enter the congestion-control command and the value *enabled*:**

   congestion-control *<enabled>*

   For example, the following command line enables congestion control for this frame relay interface:

   ```
   frame-relay/1/2# congestion-control enabled
   frame-relay/1/2#
   ```

Congestion Timer

To change the value for the congestion timer:

1. **Navigate to the prompt for the interface that you want to edit.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2
   ```

2. **Enter the congestion-timer command and the integer value you want the interface to use:**

   congestion-timer *<integer>*

   <integer> is the length of time, in seconds, during which the router counts congestion notifications (see "Congestion Counter" on page 3-62). If the router receives the number of congestion notifications you set in the congestion counter during this amount of time, the router stops transmitting data.

   Legal timer values are 0.5, 1, 1.5, 2, 2.5, 3, 3.5, 4, 4.5, and 5 seconds. The default is 1 second.

   For example, the following command line sets a congestion timer of 2.5 seconds:

   ```
   frame-relay/1/2# congestion-timer 2.5
   frame-relay/1/2#
   ```

Congestion Counter

To change the value for the congestion counter:

1. **Navigate to the prompt for the interface that you want to edit.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2;
   ```

2. **Enter the congestion-counter command and the integer value you want the interface to use:**

   congestion-counter *<integer>*

   <integer> is the maximum number of congestion notifications the router can receive during the congestion timer period before it stops transmitting data.

   Legal counter values are 1 to 500 notifications. The default is 20.

For example, the following command line sets a congestion counter of 30 notifications:

```
frame-relay/1/2# congestion-counter 30
frame-relay/1/2#
```

Congestion Method

To change the value for the congestion method:

1. **Navigate to the prompt for the interface that you want to edit.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2
   ```

2. **Enter the congestion-method command and the value you want the interface to use:**

   congestion-method *<value>*

   Legal values are:

   throttle-then-shutdown
   shutdown (the default)
   throttle

   For example, the following command line sets a congestion method of throttle:

   ```
   frame-relay/1/2# congestion-method throttle
   frame-relay/1/2#
   ```

Configuring Congestion Control for Individual SVC Options

To configure congestion control for an SVC:

Congestion Control

1. **Navigate to the prompt for the SVC option you want to edit.**

   For example:

   ```
   serial/3/2; frame-relay/3/2; service/8.0.32; svc-options/toronto
   ```

2. **Enter the congestion-control command and the value *enabled*:**

   congestion-control enabled

For example, the following command line enables congestion control for this frame relay interface:

```
svc-options/toronto# congestion-control enabled
svc-options/toronto#
```

Congestion Timer

To change the value for the congestion timer:

1. **Navigate to the prompt for the SVC that you want to edit.**

   For example:

   ```
   serial/3/2; frame-relay/3/2; service/8.0.32; svc-options/toronto
   ```

2. **Enter the congestion-timer command and the value you want the interface to use:**

   congestion-timer *<integer>*

   <integer> is the length of time, in seconds, during which the router counts congestion notifications (see "Congestion Counter" on 3-62, following). If the router receives the number of congestion notifications you set in the Congestion Counter during this amount of time, the router stops transmitting data.

   Legal timer values are 0.5, 1, 1.5, 2, 2.5, 3, 3.5, 4, 4.5, and 5 seconds. The default is 1 second.

   For example, the following command line sets a congestion timer of 2.5 seconds:

   ```
   svc-options/toronto# congestion-timer 2.5
   svc-options/toronto#
   ```

Congestion Counter

To change the value for the congestion counter:

1. **Navigate to the prompt for the SVC that you want to edit.**

   For example:

   ```
   serial/3/2; frame-relay/3/2; service/8.0.32; svc-options/toronto
   ```

2. **Enter the congestion-counter command and the value you want the interface to use:**

   congestion-counter *<integer>*

   <integer> is the maximum number of congestion notifications the router can receive during the congestion timer period before it stops transmitting data.

   Legal counter values are 1 to 500 notifications. The default is 20.

   For example, the following command line sets a congestion counter of 30 notifications:

   ```
   svc-options/toronto# congestion-counter 30
   svc-options/toronto#
   ```

Congestion Method

To change the value for the congestion method:

1. **Navigate to the prompt for the SVC that you want to edit.**

   For example:

   ```
   serial/3/2; frame-relay/3/2; service/8.0.32; svc-options/toronto
   ```

2. **Enter the congestion-method command and the value you want the interface to use:**

   congestion-method *<value>*

   Legal values are:

   throttle-then-shutdown
   shutdown (the default)
   throttle
   inherit

   For example, the following command line sets a congestion method of throttle:

   ```
   svc-options/toronto# congestion-method throttle
   svc-options/toronto#
   ```

Using Site Manager

To enable congestion control:

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on the **SVCs** button.	The Frame Relay Options List for Service window opens.
5. Choose the SVC option record that has values in the following parameters that match the remote end of the SVC connection. • **Remote Party Number** • **Remote Party SubAddress (optional)** • **Remote Party Number Plan** • **Remote Party Type of Number**	
6. Edit values for the following parameters. Use **Help** or the parameter descriptions that begin on page A-51. • **Congestion Disable** • **Congestion Timer** • **Congestion Counter** • **Congestion Method** (applies only when you enable traffic shaping)	
7. Edit other parameters if you want, and click on **Apply**.	
8. When you are finished, click on **Done**.	You return to the Frame Relay Service List window.
9. Click on **Done**.	You return to the main Configuration Manager window.

Using Traffic Shaping with SVCs

To use traffic shaping, you set attributes or parameters specific to throughput, committed burst, and excess burst. To enhance the effectiveness of traffic shaping, you may also want to edit values for the SVC Congestion Control and Congestion Method attributes or parameters. For more information about the interaction between these elements and traffic shaping, see "Traffic Shaping Considerations" in Chapter 2.

You can use either the BCC or Site Manager to shape traffic with SVCs.

Using the BCC

To configure traffic shaping you set values for committed burst, excess-burst, CIR, and traffic shaping.

Committed Burst

The committed burst rate (B_c) defines the number of bits the router can transmit over a specified time interval when congestion occurs. For SVCs you configure two attributes to define committed burst: *committed-burst-in* and *committed-burst-out*. These are, respectively the maximum number of bits that a VC can receive and transmit during the VC's burst period when congestion is occurring. To enable traffic shaping, these attributes and the CIR attributes must be greater than zero. The values in the committed burst attributes should be lower than the CIR attributes.

To change the value for committed-burst-in or committed-burst-out:

1. **Navigate to the prompt for the SVC that you want to edit.**

   For example:

   ```
   serial/1/2; frame-relay/1/2; service/8.0.32; svc-options/toronto
   ```

2. **Enter the committed-burst-in command and the integer value you want the PVC to use:**

   committed-burst-in *<integer>*

   or

   committed-burst-out *<integer>*

   <integer> is the number of bits the router can transmit per time interval.

   Legal values are 0 to 2,147,483,647 bits. The default is 0.

For example, the following command line sets a committed burst in value of 4,000 bits.

```
svc-option/tronto# committed-burst-in 4000
svc-option/tronto#
```

Excess Burst

For SVCs you configure two attributes to define excess burst: *excess-burst-in* and *excess-burst-out*. The values for excess-burst-in combined with committed-burst-in, and for excess-burst-out combined with committed-burst-out define, respectively, the maximum number of bits that a VC can receive and transmit during the VC's burst period when no congestion is occurring. The excess burst plus the committed burst must be less than or equal to the line speed:

To change the value for excess-burst-in or excess-burst-out:

1. **Navigate to the prompt for the SVC that you want to edit.**

   For example:

   ```
   serial/1/2; frame-relay/1/2; service/8.0.32; svc-options/toronto
   ```

2. **Enter the excess-burst-in or excess-burst-out command and the integer value you want the SVC to use:**

   excess-burst-in *<integer>*

   or

   excess-burst-out *<integer>*

   <integer> is the number of bits the router can transmit per time interval.

   Legal values are 0 to 2,147,483,647 bits. The default is 0.

   For example, the following command line sets a excess burst in value of 3,000 bits:

   ```
   svc-option/tronto# excess-burst-in 3000
   svc-option/tronto#
   ```

CIR (Throughput)

The CIR (committed information rate), or throughput, defines the number of bits per second your carrier guarantees the router can transmit over a specified time interval when there is no congestion. For SVCs, you configure four attributes that define throughput: cir-in, cir-in-minimum, cir-out, and cir-out-minimum.

The *cir-in* and *cir-out* attributes specify the requested incoming and outgoing throughput (kbits/second) when no congestion is occurring.

The *cir-in-minimum* and *cir-out-minimum* attributes specify the minimum acceptable incoming and outgoing throughput (kbits/second).

To change the value of the cir-in or cir-out attributes:

1. **Navigate to the prompt for the SVC that you want to edit.**

   For example:

   ```
   serial/1/2; frame-relay/1/2; service/8.0.32; svc-options/toronto
   ```

2. **Enter the cir-in or cir-out command and the integer value you want the SVC to use:**

   cir-in *<integer>*

   or

   cir-out *<integer>*

   <integer> is the number of bits the router can transmit per time interval.

   Legal values are 0 to 2,147,483,647 bits. The default is 0.

   For example, the following command line sets a cir-in value of 10,000 bits:

   ```
   svc-option/tronto# cir-in 10000
   svc-option/tronto#
   ```

To change the value of the cir-in-minimum or cir-out-minimum attribute:

1. **Navigate to the prompt for the SVC that you want to edit.**

   For example:

   ```
   serial/1/2; frame-relay/1/2; service/8.0.32; svc-options/toronto
   ```

2. **Enter the cir-in-minimum or cir-out-minimum command and the integer value you want the SVC to use:**

   cir-in-minimum *<integer>*

   or

   cir-out-minimum *<integer>*

   <integer> is the number of bits the router can transmit per time interval.

   Legal values are 0 to 2,147,483,647 bits. The default is 0.

For example, the following command line sets a cir-in-minimum value of 10,000 bits:

```
svc-option/tronto# cir-in-minimum 10000
svc-option/tronto#
```

Traffic Shaping Control

To use traffic shaping for SVCs you set the **traffic-shaping-control** command to enabled, but you also have these options:

- If you do not want to use traffic shaping on this SVC, accept the default, *disabled*, and do not set the CIR, committed burst, and excess burst attributes.
- To use traffic shaping and accept the quality of service (QoS) the network provides, set this attribute to *enabled*, and do not configure the CIR, committed burst, and excess burst attributes.
- To use traffic shaping, and negotiate QoS with the network, set this command to *enabled*, and also set the CIR, committed burst, and excess burst attribute attributes.
- To prevent the router from enforcing the CIR, set this command to *disabled*, and also set the CIR, committed burst, and excess burst attributes.

To set this command:

1. **Navigate to the prompt for the SVC that you want to edit.**

   For example:

   ```
   serial/1/2; frame-relay/1/2; service/8.0.32; svc-options/toronto
   ```

2. **Enter the traffic-shaping-control command and set the value to *enabled*:**

   Legal values are **enabled** and **disabled**. The default is disabled.

   For example, the following command line enables traffic shaping on this SVC:

   ```
   svc-option/tronto# traffic-shaping-control enabled
   svc-option/tronto#
   ```

Using Site Manager

To enable traffic shaping:

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Choose the service record that includes the SVC that you want to configure for traffic shaping.	
5. Click on the **SVCs** button.	The Frame Relay SVC Options List for Service window opens.
6. Choose the SVC option record that has values in the following parameters that match the remote end of the SVC connection. Use **Help** or the parameter descriptions that begin on page A-41: • **Remote Party Number** • **Remote Party SubAddress (optional)** • **Remote Party Number Plan** • **Remote Party Type of Number**	
7. Set the **Traffic Shaping Disable** parameter to **Enable**.	
8. To define traffic shaping values for this SVC, edit the following parameters. Use **Help** or the parameter descriptions that begin on page A-48. • **LL Core Out Throughput (CIR)** • **LL Core In Throughput (CIR)** • **LL Core Min Out Throughput** • **LL Core Min In Throughput** • **LL Core Out Committed Burst** • **LL Core In Committed Burst** • **LL Core Out Excess Burst** • **LL Core In Excess Burst** • **Traffic Shaping Disable**	
9. Click on **Apply**.	

Site Manager Procedure *(continued)*	
You do this	**System responds**
10. Click on **Done**.	You return to the Frame Relay SVC Options List window.
11. When you are finished, click on **Done**.	You return to the Frame Relay Service List window.
12. Click on **Done**.	You return to the main Configuration Manager window.

Using Data Compression with SVCs

You can use the BCC or Site Manager to set data compression for SVCs.

Using the BCC

The default option for the **wcp-control** command is **enabled**. To disable compression for this VC:

1. **Navigate to the prompt for the SVC that you want to edit.**

   For example:

   ```
   box; serial/1/2; frame-relay/1/2; svc-options/toronto
   ```

2. **Enter the wcp-control command and the value *disabled*:**

   For example, the following command line disable compression for this VC.

   ```
   svc-options/toronto# wcp-control disabled
   svc-options/toronto#
   ```

Using Site Manager

To use data compression with frame relay SVCs, first select WCP from the Protocols menu. Compression is enabled by default for individual SVCs, so you do not have to set this WCP Enable parameter to use compression. For information on setting WCP parameters, see *Configuring Data Compression Services*.

To disable compression:

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Choose the service record that you want to configure for compression.	
5. Click on the **SVCs** button.	The Frame Relay Options List for Service window opens.
6. Choose the SVC option record that has values in the following parameters that match the remote end of the SVC connection. • **Remote Party Number** • **Remote Party SubAddress (optional)** • **Remote Party Number Plan** • **Remote Party Type of Number**	
7. Set the **WCP Enable** parameter to Disable.	
8. Click on **Apply**.	
9. Click on **Done**.	You return to the Frame Relay Service List window.
10. Click on **Done**.	You return to the main Configuration Manager window.

Setting X.213 Priorities for SVCs

Some frame relay networks can prioritize SVC data and connection characteristics by setting X.213 priority attributes or parameters. While you configure them at the router, it is the network that uses these values.

You can use either the BCC or Site Manager to set X.213 priorities for SVCs.

Using the BCC

The X.213 priority commands adhere to ITU-T Q.933 and X.213. They are data-priority, data priority-minimum, gain-priority, gain-priority-minimum, keep-priority, and keep-priority-minimum. If your network does not support X.213 prioritization, accept the default values for these commands, unless the network is able to accept pieces of signaling information that it does not recognize.

The *data-priority* commands sets the priority of data on the network connection. It is a value the router requests; it is not guaranteed. The *data-priority-minimum* command sets the lowest acceptable priority of data on a connection.

The *gain-priority* commands sets the priority of data required to add a connection. it is a value the router requests; it is not guaranteed. The *gain-priority-minimum* command sets the lowest acceptable priority of data to add a connection. This is a value below which the router will not create the SVC.

The *keep-priority* command sets the priority of data required to maintain a connection. This is a value the router requests; it is not guaranteed. The *keep-priority-minimum* command sets the lowest acceptable priority of data required to maintain a connection. This is a value below which the router will disconnect the SVC.

To set X.213 priority values:

1. **Navigate to the prompt for the SVC that you want to edit.**

   For example

   ```
   box; serial/1/2; frame-relay/1/2; svc-options/toronto
   ```

2. **Enter the command for the attribute you want to edit, and the value you want the attribute to use. The options are:**

   data-priority *<integer>*
   data-priority-minimum *<integer>*
   gain-priority *<integer>*
   gain-priority-minimum *<integer>*
   keep-priority *<integer>*
   keep-priority-minimum *<integer>*

   The *<integer>* for all of these attributes is 0 to 15, with 0 as the lowest priority, and 14 as the highest. A value of 15 means unspecified.

For example, the following command line sets a data-priority of 9 for SVC options:

```
svc-options/toronto# data-priority 9
svc-options/toronto#
```

Using Site Manager

To set X.213 priority values:

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Choose the service record that includes the SVC that you want to configure for traffic shaping.	
5. Click on the **SVCs** button.	The Frame Relay SVC Options List for Service window opens.
6. Choose the SVC option record that has values in the following parameters that match the remote end of the SVC connection. • **Remote Party Number** • **Remote Party SubAddress (optional)** • **Remote Party Number Plan** • **Remote Party Type of Number**	
7. Set the following parameters, using **Help** or the parameter descriptions that begin on page A-45. • **X.213 Data Priority** • **X.213 Data LQA Priority** • **X.213 Gain Priority** • **X.213 Gain LQA Priority** • **X.213 Keep Priority** • **X.213 Keep LQA Priority**	
8. Click on **Apply**.	Your changes take effect.

Site Manager Procedure *(continued)*	
You do this	**System responds**
9. Click on **Done**.	You return to the Frame Relay Service List window.
10. Click on **Done**.	You return to the main Configuration Manager window.

Deleting Frame Relay

To delete frame relay from a circuit on which it is currently configured:

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Choose circuit, click on **Delete**.	Circuit List window opens.
4. Choose circuit, click on **Delete**.	Delete Circuit window opens.
5. Click on **Delete**.	The Frame Relay List window opens.
6. Click on **Done**.	The Configuration Manager window opens.

To delete frame relay from *all* circuits on which it is currently configured:

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.

Site Manager Procedure	
You do this	**System responds**
3. Click on **Delete Frame Relay**.	A confirmation window prompts "`Do you REALLY want to delete Frame Relay?`"
4. Click on **OK**.	The confirmation window closes, revealing the Configuration Manager window.

Appendix A
Site Manager Parameters

These topics define frame relay parameters:

Topic	Page
Interface Parameters	A-1
SVC LAPF Parameters	A-11
Parameters for PVCs	A-22
SVC Service Record Parameters	A-34

Interface Parameters

The Frame Relay Interface List window contains the parameters for the frame relay interfaces. If you have configured PVCs only, you see a window similar to the one in Figure A-1.

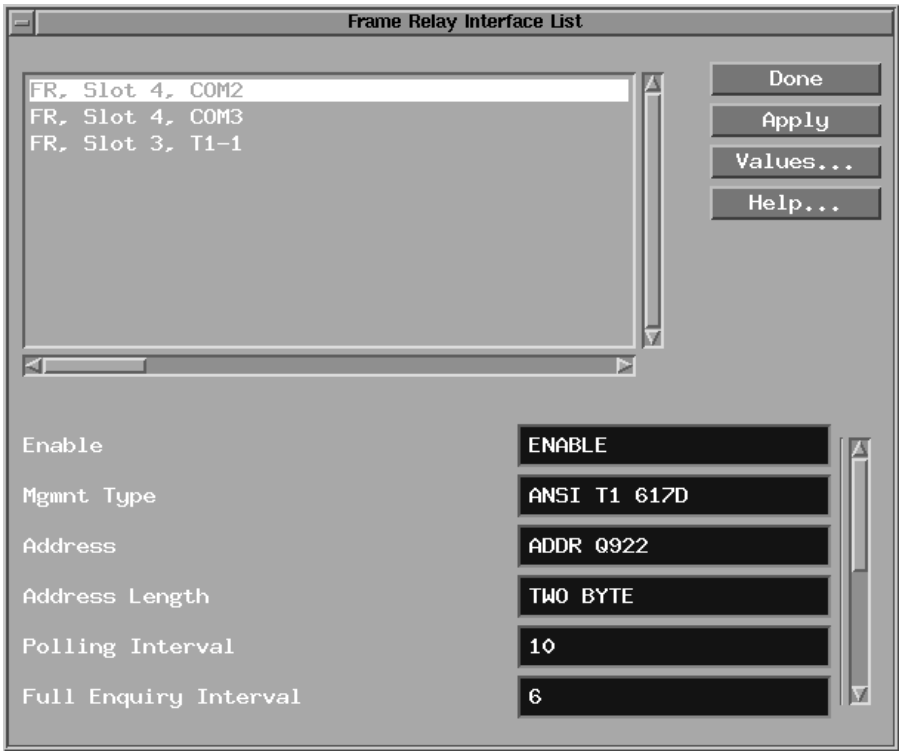

Figure A-1. Frame Relay Interface List Window (for PVCs)

If you have configured any SVCs, you see a window similar to the one in Figure A-2, which includes buttons for LAPF and Signaling.

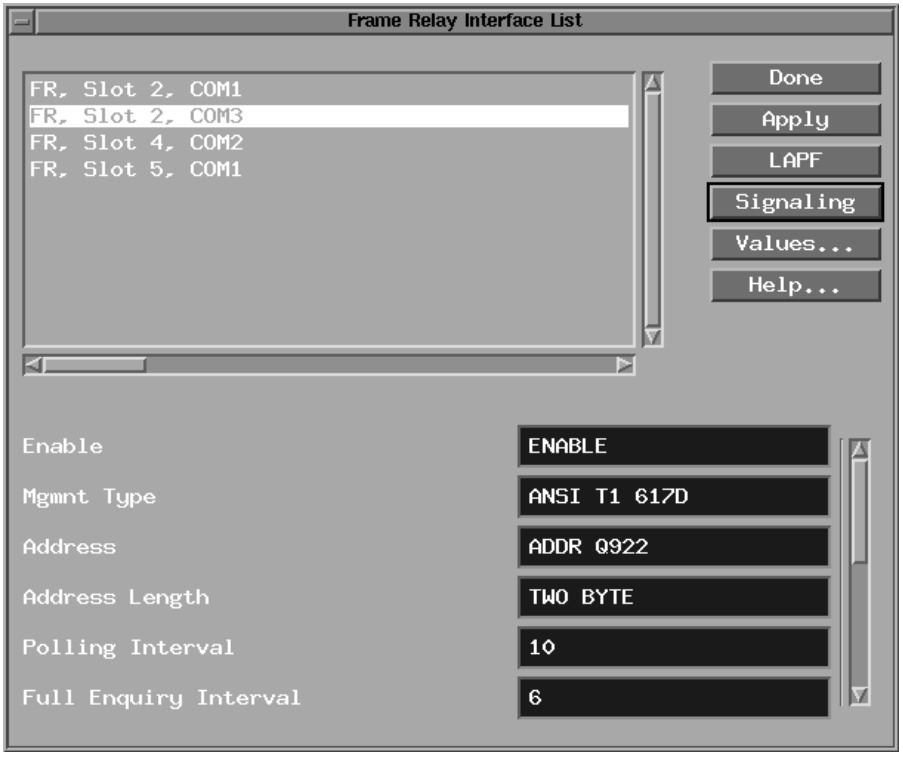

Figure A-2. Frame Relay Interface List Window (for SVCs)

To access the Frame Relay Interface List window:

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Interfaces**.	The Frame Relay Interface List window opens.

Descriptions of Interface Parameters

Frame Relay Interface parameters are the same for PVCs and SVCs. Use the descriptions that follow when you edit these parameters.

Parameter: Enable

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: Enable

Options: Enable | Disable

Function: Enables or disables frame relay service on this port.

Instructions: To disable frame relay service on this interface without deleting it, set to Disable. To reenable frame relay service, if you previously disabled it, set to Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.2

Parameter: Mgmnt Type

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: ANSI T1.617D

Options: DLCMI None │ Rev 1 LMI │ ANSI T1.617D │ CCITT Annex A │ LMI Switch │ Annex D Switch │ Annex A Switch

Function: Specifies the management protocol that the router and the frame relay network use to communicate status information. Routers connected back to back also use a management protocol to exchange status information.

Option for No Management

DLCMI None - provides no management interface between the router and the frame relay network. In the absence of management support, you must configure all PVCs manually.

Options for User Management

Rev 1 LMI - provides user-side management services as specified by Revision 1 of the Local Management Interface standard.

ANSI T1.617D - provides user-side management services as specified in Annex D to ANSI standard T1.617-1991.

CCITT Annex A - provides user-side management services as specified by the ITU-T (formerly CCITT).

Options for Limited Management for DCE Switch (primarily for troubleshooting)

LMI Switch - offers limited management services for the DCE side of the connection as specified by Revision 1 of the Local Management Interface standard.

Annex D Switch - provides limited management services for the DCE side of the connection as specified in Annex D to ANSI standard T1.617-1991.

Annex A Switch - provides limited management services for the DCE side of the connection as specified by the ITU-T.

Instructions: Select the management protocol for the frame relay network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.6

Parameter: **Address**

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: ADDR Q922

Options: ADDR Q922 | ADDR Q922 November 90 | ADDR Q922 MARCH 90 | ADDR Q921

Function: Specifies the DLCI addressing type.

ADDR Q922 - selects addressing as specified in the final version of the Q.922 standard. Q.922 provides for FECN, BECN, DE, and EA bits. While most Q.922 addresses are included within a 2-octet field, the standard allows for 3- and 4-octet address fields.

The November draft of ADDR Q922 - differs from ADDR Q922 in dropping the D/C bit from the extended (3- and 4-byte) forms.

The March draft of ADDR Q922 - differs from ADDR Q922 in defining an 11-bit DLCI and dropping the DE bit from the second octet of the address field.

ADDR Q921 - differs from ADDR Q922 MARCH 90 in that it does not use FECNs or BECNs.

Instructions: Select the addressing type for the frame relay interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.8

Parameter: **Address Length**

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: Two Byte

Options: Two Byte | Three Byte | Four Byte

Function: Specifies the length of the frame relay address field.

The length of this field determines the range of valid numbers for the DLCI number set in the Frame Relay PVC List window. For more details, see the DLCI Number parameter description on page A-25.

Instructions: Select the address length for the address field. This must match what the network specifies.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.9

Parameter: Polling Interval

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: 10

Options: 5 to 30 seconds

Function: Specifies the interval between status inquiry messages that the router transmits. Status inquiry messages cause a network response in the form of a link integrity verification message or full status message. Successful completion of the request/response "handshake" verifies the status of the router/frame relay network link.

Instructions: You should accept the default value, 10 seconds. If this value does not match what the network requests, enter a value that is appropriate for your network in the range of 5 to 30 seconds. Polling Interval does not function if you set Mgmnt Type to DLCMI None.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.10

Parameter: Full Enquiry Interval

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: 6

Options: 1 to 255 polling intervals

Function: Specifies the interval between full status inquiry messages that the router transmits. Full status inquiry messages cause the network to send a full status report message, which lists all PVCs, the PVC status (active or inactive, and new or previously established). This parameter works with the Polling Interval parameter.

The default value, 6, tells the router to send a full status inquiry every 6 polling intervals. For example, with a polling interval of 10 and a full enquiry interval of 6, the router transmits a full status inquiry every 60 seconds; with a polling interval of 20 and a full enquiry interval of 30, the router transmits a full status inquiry every 10 minutes (600 seconds).

Instructions: Enter a value from 1 to 255, according to what the network dictates. Full Enquiry Interval does not function if you set Mgmnt Type to DLCMI None.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.11

Parameter: Error Threshold

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: 3

Options: 0 to 2,147,483,647

Function: Together with the value of the Monitored Events parameter, establishes a criterion to evaluate the quality of the router/frame relay network connection.

If you accept the default values for both Error Threshold and Monitored Events, three status exchange errors in a sequence of four attempted exchanges will bring the connection down. With Error Threshold set to 5 and Monitored Events set to 10, five status exchange errors in a continuous sequence of 10 attempted exchanges will bring the connection down.

After the network clears the connection, status exchanges continue, and the router monitors line integrity. When the number of consecutive, successful status exchanges is equal to the Error Threshold value, the router restores the frame relay connection.

Error Threshold and Monitored Events are nonfunctional if you set Mgmnt Type to DLCMI None.

Instructions: Enter the number of faulty status exchanges that will bring the connection down.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.12

Parameter: Monitored Events

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: 4

Options: 0 to 2,147,483,647 events

Function: Together with the value of the Error Threshold parameter, establishes a criterion to evaluate the quality of the router/frame relay network connection. See the description of the Error Threshold parameter for more information.

Instructions: Enter the number of consecutive status exchanges you want the router to monitor.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.13

Parameter: Multicast

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: Disable

Options: Enable │ Disable

Function: Enables or disables support for frame relay multicast service.

Instructions: If your frame relay subscription service provides multicast service, and if this frame relay interface should receive multicast messages, set to Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.16

Parameter: Congestion Control

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: Disable

Options: Enable │ Disable

Function: Enables or disables congestion control on this interface. A value of Enable tells the router to drop all outbound traffic destined for a PVC where congestion is occurring until the congestion clears. The value of this parameter affects all PVCs that you do not individually configure.

Instructions: To activate congestion control, set to Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.22

Parameter: Congestion Timer

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: 1

Options: 0.5 to 5 seconds, in 0.5-second intervals

Function: Specifies the length of time, in seconds, during which the router counts congestion notifications. If the router receives the number of congestion notifications set by the congestion counter parameter, the router stops transmitting data. The router resumes transmission once it stops receiving congestion notifications.

Instructions: Set the length of time the router should count congestion notifications from the network. If you set this parameter for a long time period, the router may be less likely to stop transmission for an intermittent congestion condition. However, the router may be slow to detect congestion, resulting in long transmission delays once the congestion has cleared. The value of this parameter applies to all PVCs that you do not individually configure.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.23

Parameter: Congestion Counter

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: 20

Options: 1 through 500 notifications

Function: Indicates the maximum number of congestion notifications that the router can receive during the congestion timer period before it stops transmitting. If the router reaches the value set by this parameter, it determines the line is congested and stops transmitting.

Instructions: Specify the congestion count. The smaller the number, the more quickly the router detects congestion and stops transmitting. The value of this parameter applies to all PVCs that you do not individually configure.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.24

Parameter:	**Congestion Method**
Path:	Configuration Manager > Protocols > Frame Relay > Interfaces
Default:	Shutdown
Options:	Shutdown │ Throttle │ Throttle Then Shutdown
Function:	Specifies the method of congestion control: • Shutdown - terminates the VC when congestion occurs. • Throttle - queues traffic when congestion occurs; traffic resumes when congestion alleviates. This option is valid only when traffic shaping is enabled. • Throttle Then Shutdown - first queues traffic when congestion occurs, and then terminates the VC if throttling does not alleviate congestion. This option is valid only when traffic shaping is enabled.
Instructions:	Select a setting appropriate to your network.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.9.2.1.18

SVC LAPF Parameters

If you configure SVCs, LAPF parameters are important to your network. You can edit these parameters in the Frame Relay LAPF Parameters window (Figure A-3).

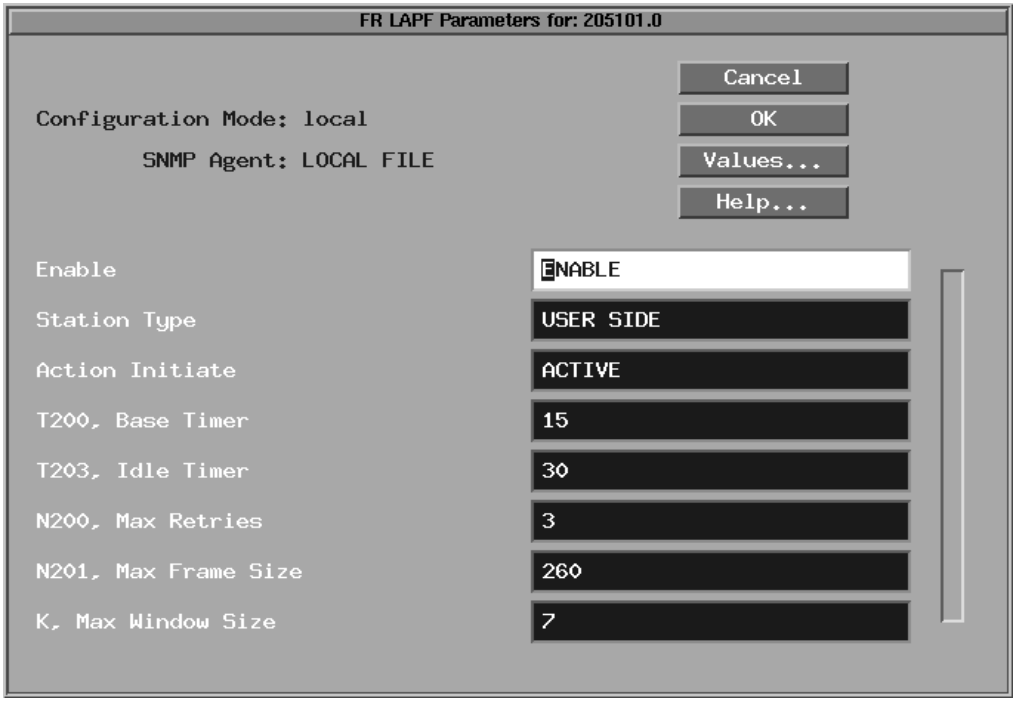

Figure A-3. FR LAPF Parameters Window

To access the FR LAPF Parameters window:

Site Manager Procedure	
You do this	**System responds**
1. Click on the Protocols menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Interfaces**.	The Frame Relay Interface List window opens.
4. Click on the **LAPF** button.	The Frame Relay LAPF Parameters window opens.

Parameter: Enable

Path: Configuration Manager > Protocols > Interfaces > LAPF

Default: Enable

Options: Enable | Disable

Function: Enables or disables LAPF on this interface.

Instructions: To disable LAPF on this interface, set to Disable. To enable LAPF, accept the default, Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.7.1.2

Parameter: Station Type

Path: Configuration Manager > Protocols > Interfaces > LAPF

Default: User Side

Options: Network Side | User Side

Function: Identifies the desired station type of this interface.

Network Side indicates that LAPF will act as the data communications equipment.

User Side indicates that LAPF will act as the data terminal equipment.

Instructions: To have LAPF act as the DTE, accept the default, User Side. To have LAPF act as the DCE, set to Network Side.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.7.1.6

Parameter:	**Action Initiate**
Path:	Configuration Manager > Protocols > Interfaces > LAPF
Default:	Active
Options:	Active | Passive
Function:	Identifies the action LAPF will take to initiate link setup by sending or holding unnumbered command (SABME) frames to poll the router at the other end of the connection. Active indicates that LAPF will *send* SABME frames and initiate link setup. Passive indicates that LAPF will *hold* SABME frames and take no action to initiate link setup. To establish a LAPF link, at least one end of the connection has to initiate link setup.
Instructions:	To have LAPF initiate link setup from this router, accept the default, Active. To have LAPF take no action to initiate link setup, set to Passive.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.9.7.1.7

Parameter: **T200, Base Timer**

Path: Configuration Manager > Protocols > Interfaces > LAPF

Default: 15

Options: 1 to 1200 tenths of a second

Function: Indicates the amount of time (in tenths of a second) that the router waits to receive an acknowledgment from its remote peer.

This timer is the general purpose retransmission timeout. It is used during initiation of LAPF multiple frame support and for timeout of LAPF numbered information frames.

During initiation of LAPF multiple frame support, an unnumbered command (SABME) frame is sent to the peer LAPF to request multiple frame communications on the link. The peer LAPF responds with an unnumbered acknowledgment (UA) frame.

When multiple frame support has been established, numbered command/response information (I) frames are transmitted both ways across the connection. These I frames carry an acknowledgment of the highest number frame received by the sending LAPF.

In the event of a timeout, the sending platform retransmits the frame, up to the maximum number of times specified by the N200, Max Retries parameter.

Instructions: Set to the retransmission timeout value appropriate for your network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.7.1.8

Parameter: **T203, Idle Timer**

Path: Configuration Manager > Protocols > Interfaces > LAPF

Default: 30

Options: 1 to 120 seconds

Function: Indicates the amount of time (in seconds) that the router allows for idle time with no data being transmitted. In the event of a timeout, the router initiates a frame handshake to check if the connection is still up.

Instructions: Set to the idle time value appropriate for your network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.7.1.9

Parameter: N200, Max Retries

Path:	Configuration Manager > Protocols > Interfaces > LAPF
Default:	3
Options:	1 to 20
Function:	Indicates the maximum number of LAPF retransmissions allowed on a connection after the T200 Base Timer expires before the connection terminates.
Instructions:	Set to the value of retransmissions appropriate for your network.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.9.7.1.10

Parameter: N201, Max Frame Size

Path:	Configuration Manager > Protocols > Interfaces > LAPF
Default:	260
Options:	260 to 2052 octets
Function:	Indicates the maximum number of octets of data allowed in the LAPF information field. The larger the number allowed, the less overhead on the system. However, a large value could exceed the system buffer size. You should accept the default value.
Instructions:	Set to the maximum size of the LAPF information field.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.9.7.1.11

Parameter: K, Max Window Size

Path:	Configuration Manager > Protocols > Interfaces > LAPF
Default:	7
Options:	1 to 127
Function:	Indicates the maximum number of outstanding numbered information (I) frames allowed across a connection. These are frames that have travelled across the link, but which the peer has not acknowledged. Each of these frames remains in a backup queue until the peer sends an acknowledge message. A longer queue adversely affects system performance. You should accept the default value.
Instructions:	Set to the value appropriate for your network.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.9.7.1.12

SVC Signaling Parameters

If you configure SVCs, signaling parameters are important to your network. You can edit these parameters in the Frame Relay Signaling Parameters window (Figure A-4).

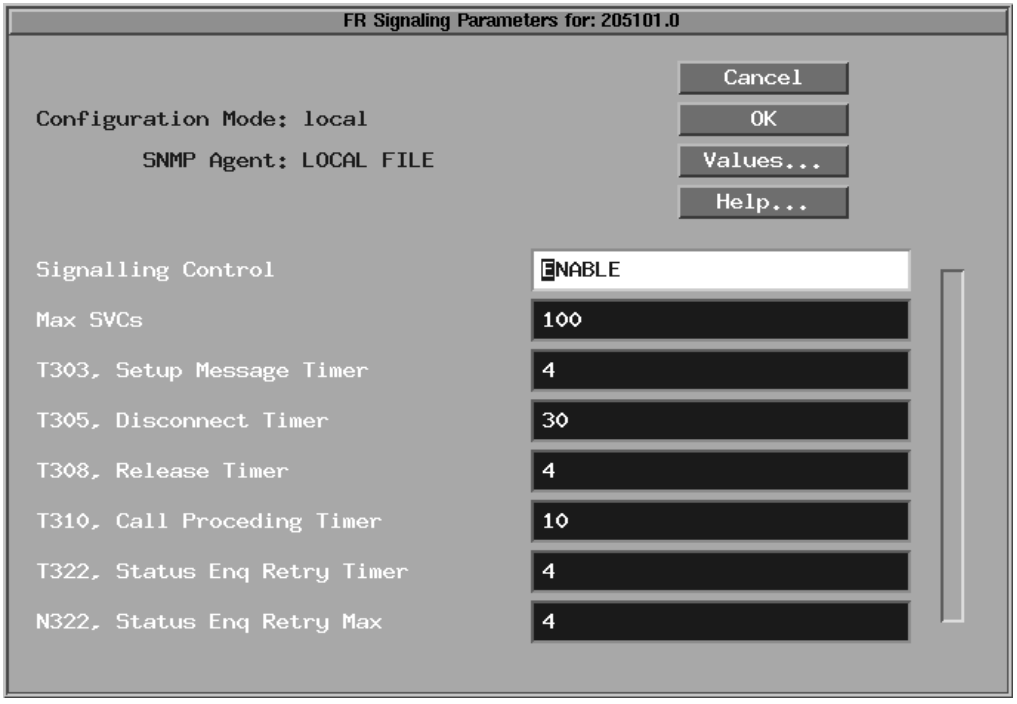

Figure A-4. Frame Relay Signaling Parameters Window

To access the Frame Relay Signaling Parameters window:

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Interfaces**.	The Frame Relay Interface List window opens.
4. Click on the **Signaling** button.	The Frame Relay Signaling Parameter window opens.

Parameter: Signaling Control

Path: Configuration Manager > Protocols > Frame Relay > Interfaces > Signaling

Default: Enable

Options: Enable | Disable

Function: Enables or disables signaling on this interface.

Instructions: To use signaling on the interface, accept the default, Enable. If you do not want to use signaling, choose Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.9.1.2

Parameter: Max SVCs

Path: Configuration Manager > Protocols > Interfaces > Signaling

Default: 100

Options: 1 to 2147483647

Function: Indicates the maximum number of simultaneous switched virtual circuits allowed on the port. The more SVCs you allow on the port, the larger the system memory required to support them.

Instructions: Enter the maximum number of simultaneous SVCs per port for your network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.9.1.5

Parameter: **T303, Setup Message Timer**

Path: Configuration Manager > Protocols > Frame Relay > Interfaces > Signaling

Default: 4

Options: 2 to 90 seconds

Function: Indicates the number of seconds allowed from the time the router sends a setup message to the called subscriber and receives a connect or call proceeding message from the called subscriber.

In the event of a timeout, the router retransmits the setup message and restarts the timer. If the timer expires a second time, the call is cleared.

Instructions: Enter the timer value for call setup.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.9.1.6

Parameter: **T305, Disconnect Timer**

Path: Configuration Manager > Protocols > Frame Relay > Interfaces > Signaling

Default: 30

Options: 20 to 90 seconds

Function: Indicates the number of seconds allowed from the time the router sends a disconnect message and receives a release message back. This timer is used when this router initiates call clearing.

In the event of a timeout, the router sends a release message and enters the release request state. The timer is not restarted.

Instructions: Enter the timer value for call clearing.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.9.1.7

Parameter: **T308, Release Timer**

Path: Configuration Manager > Protocols > Frame Relay > Interfaces > Signaling

Default: 4

Options: 2 to 90 seconds

Function: Indicates the number of seconds allowed for call clearing initiated by the other end of the connection or when the T305 Disconnect Timer expires.

- If timer T305 expires, the router enters the release request state, starts timer T308, and sends a release message.
- Timer T308 stops when the router receives a release complete message from the other end of the connection.

In the event of a timeout, the router retransmits the release message and restarts the timer. If the timer expires a second time, the call is cleared. The timer is not restarted.

Instructions: Enter the timer value for call clearing by the other end of the connection, or when timer T305 expires.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.9.1.8

Parameter: **T310, Call Proceding Timer**

Path: Configuration Manager > Protocols > Frame Relay > Interfaces > Signaling

Default: 10

Options: 2 to 90 seconds

Function: Indicates the number of seconds allowed from the time the router receives a call proceeding message to the time the router receives and a connect or disconnect message.

In the event of a timeout, the router clears the call. The timer is not restarted.

Instructions: Enter the timer value for call proceeding.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.9.1.9

Parameter: **T322, Status Enq Retry Timer**

Path: Configuration Manager > Protocols > Frame Relay > Interfaces > Signaling

Default: 4

Options: 2 to 90 seconds

Function: Indicates the number of seconds allowed from the time the router sends a status inquiry message to the time the router receives an incoming status, disconnect, release, or release complete message.

If a timeout occurs, the router retransmits the status inquiry and restarts the timer. This occurs for the number of times set in the N322, Status Enq Retry Max parameter (see the next parameter), after which the call will be cleared.

Instructions: Enter the timer value for status inquiries.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.9.1.10

Parameter: **N322, Status Enq Retry Max**

Path: Configuration Manager > Protocols > Frame Relay > Interfaces > Signaling

Default: 4

Options: 1 to 20

Function: Indicates the maximum number of times the router will retransmit a status inquiry message.

If the router sends the maximum number of status inquiry messages and receives no response, the call is cleared.

Instructions: Enter a value for status inquiry retries.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.9.1.11

Parameters for PVCs

The following topics give information about configuring PVCs:

Topic	Page
Service Name Parameter	A-22
Required DLCI Parameter for Each PVC	A-24
PVC Service Record Parameters	A-26
Optional Algorithm Parameter for Each Multiline Configuration	A-32

Service Name Parameter

The Frame Relay Service List window (Figure A-5) contains the Service Name parameter, and the PVCs button that opens the PVC List for Service window where you can edit PVC parameters.

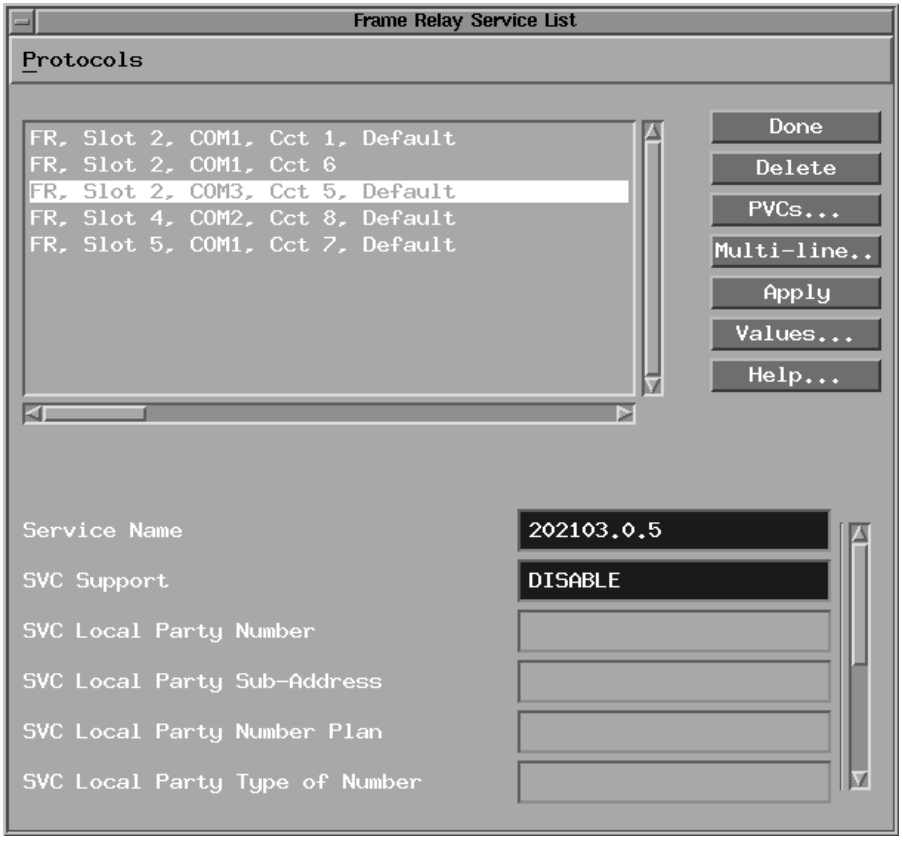

Figure A-5. Frame Relay Service List Window (for PVCs)

To access the Frame Relay Service List window:

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.

Parameter:	**Service Name**
Path:	Configuration Manager > Protocols > Frame Relay > Services
Default:	None
Options:	<*line number*>.0.<*circuit number*>
Function:	Identifies the service record.
Instructions:	Site Manager assigns a unique name in the format given to each service record. There is no need to change this value.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.9.5.1.7

Required DLCI Parameter for Each PVC

The Frame Relay PVC Add window (Figure A-6) contains the DLCI Number parameter.

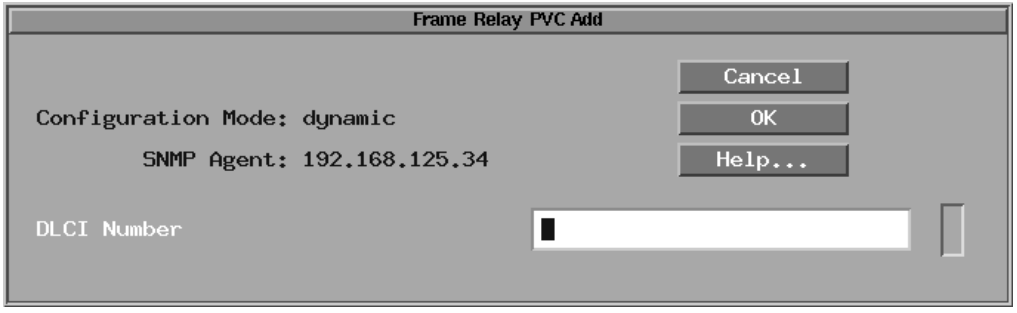

Figure A-6. Frame Relay PVC Add Window

To access the Frame Relay PVC Add window:

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on the **PVCs** button.	The FR PVC List for Service window opens.
5. Click on the **Add** button.	The Frame Relay PVC Add window opens.

Parameter: DLCI Number

Path: Configuration Manager > Protocols > Frame Relay > Services > PVCs > Add

Default: None

Options: The frame relay switch provider assigns DLCI numbers. These assigned numbers are valid options.

Valid DLCI numbers vary based on the frame relay address length. The DLCI numbers that the switch provider assigns are generally in the following ranges:

2 byte -- 16 to 1007
3 byte -- 1024 to 64511
4 byte -- 131072 to 4194303

Function: Specifies the PVC identification number that the frame relay network uses to direct data.

Instructions: Enter the decimal number that the frame relay provider assigns.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.4

PVC Service Record Parameters

The FR PVC List for Service window (Figure A-7) contains the PVC parameters set automatically when you use the Add button to add a PVC.

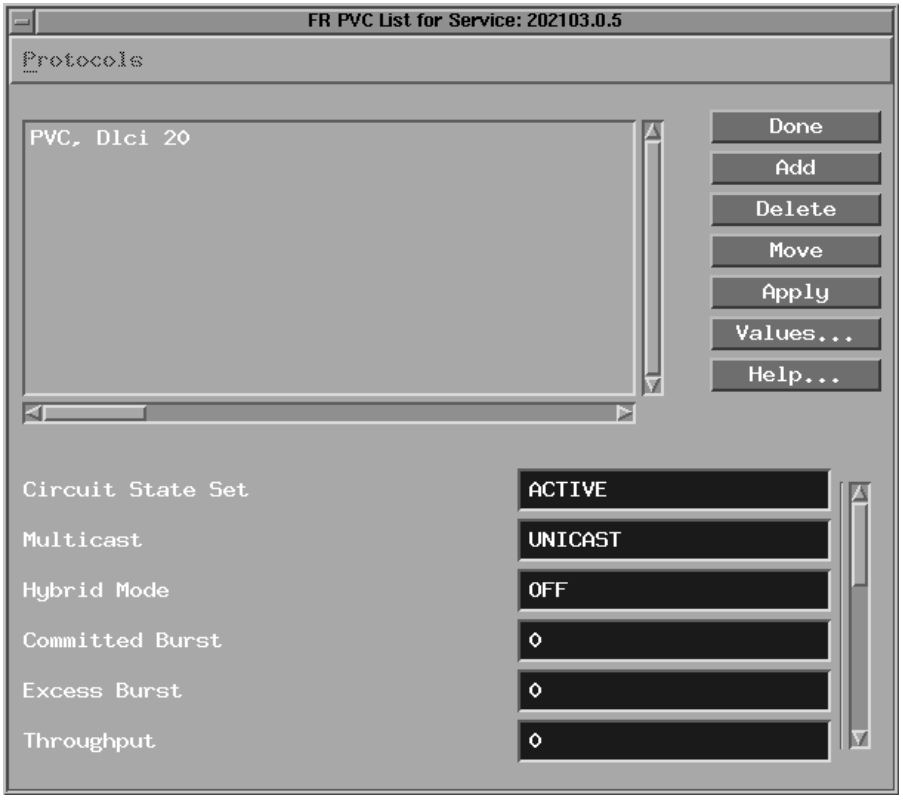

Figure A-7. FR PVC List for Service Window

To access the FR PVC List for Service window:

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on the **PVCs** button.	The FR PVC List for Service window opens.

Parameter: Circuit State Set

Path: Configuration Manager > Protocols > Frame Relay > Services > PVCs

Default: Active

Options: Invalid │ Active │ Inactive

Function: Specifies the state of the PVC.

Instructions: To indicate to a frame relay switch that the PVC is available for use, set to Active. To indicate that the PVC is configured, but not available for use (for example, before your switch provider actually activates the PVC), set to Inactive. If the PVC is configured, but the switch is unaware of it, choose Invalid.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.7

Parameter: Multicast

Path: Configuration Manager > Protocols > Frame Relay > Services > PVCs

Default: Unicast

Options: Unicast │ Multicast

Function: Indicates whether this PVC is multicast or unicast.

Instructions: Set to Unicast or Multicast according to PVC type, as the frame relay switch provider instructs.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.19

Parameter: Hybrid Mode

Path: Configuration Manager > Protocols > Frame Relay > Services > PVCs
Default: OFF
Options: ON | OFF
Function: Allows you to use the same PVC for both routing and bridging.
Instructions: If you do not want to enable both routing and bridging services, accept the default, OFF. If you do want to enable both routing and bridging, set to ON.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.1.2.1.24

Parameter: Committed Burst

Path: Configuration Manager > Protocols > Frame Relay > Services > PVCs
Default: 0
Options: 0 to 2,147,483,647 bits
Function: The maximum number of bits that a VC can transmit during the VC's burst period (Tc) when congestion is occurring. To enable traffic shaping, this parameter and the Throughput parameter (CIR) must both be greater than zero. The Committed Burst (Bc) value should be lower than the Throughput.
Instructions: Enter a value within the given range. You should set this parameter to 1/4 of the CIR unless this VC is sending frames larger than that size. If the VC is sending large frames, increase the value of this parameter to accommodate the size of those frames.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.16

Parameter: Excess Burst

Path: Configuration Manager > Protocols > Frame Relay > Services > PVCs
Default: 0
Options: 0 to 2,147,483,647 bits
Function: This value is added to the Committed Burst value to determine the maximum number of bits that may be transmitted during the VC's burst period when there is no congestion. The Excess Burst plus the Committed Burst must be less than or equal to the line speed.
Instructions: Enter a value within the given range.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.17

Parameter: Throughput

Path: Configuration Manager > Protocols > Frame Relay > Services > PVCs

Default: 0

Options: 0 to 2,147,483,647 b/s

Function: The rate in bits per second at which data travels over this VC when no congestion is occurring. To enable traffic shaping, this parameter and the Committed Burst parameter must be set to values greater than zero.

Instructions: Your carrier supplies the CIR or throughput value, which you enter in this parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.18

Parameter: Congestion Control

Path: Configuration Manager > Protocols > Frame Relay > Services > PVCs

Default: Inherit

Options: Disable | Enable | Inherit

Function: Enables or disables congestion control on this interface.

Instructions: To activate congestion control, set to Enable. This value tells the router to drop all traffic destined for a congested PVC until the congestion clears. To deactivate congestion control, set to Disable. If you want the Congestion Control setting for this PVC to match the setting you specify for the frame relay Interface Congestion Control parameter, accept the default, Inherit.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.25

Parameter: **Congestion Timer**

Path: Configuration Manager > Protocols > Frame Relay > Services > PVCs

Default: 1

Options: 0.5 to 5 seconds, in 0.5-second intervals

Function: Specifies the length of time, in seconds, during which the router counts congestion notifications. If the router receives the number of congestion notifications set by the Congestion Counter parameter, the router stops transmitting data. The router resumes transmission once it stops receiving congestion notifications.

Instructions: Set the length of time the router should count congestion notifications from the network. If you set this parameter for a long time period, the router may be less likely to stop transmission for an intermittent congestion condition. However, the router may be slow to detect congestion, resulting in long transmission delays once the congestion has cleared.

If you set the Congestion Control parameter to Inherit, the PVC uses DLCMI for congestion control, not the value of this parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.27

Parameter: **Congestion Counter**

Path: Configuration Manager > Protocols > Frame Relay > Services > PVCs

Default: 20

Options: 1 to 500 notifications

Function: Sets the maximum number of congestion notifications that the router can receive during the Congestion Timer period before it stops transmitting.

Instructions: Specify the congestion count. The smaller the number, the more quickly the router detects congestion and stops transmitting. Note, however, that if you set the Congestion Control parameter to Inherit, the PVC uses DLCMI for congestion control, not the value of this parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.28

Parameter: **Congestion Method**

Path: Configuration Manager > Protocols > Frame Relay > Services > PVCs

Default: Inherit

Options: Shutdown │ Throttle │ Throttle Then Shutdown │ Inherit

Function: Specifies the method of congestion control:

- Inherit - specifies that this VC will use the value of the interface Congestion Method parameter.
- Shutdown - terminates the VC when congestion occurs.
- Throttle - queues traffic when congestion occurs; traffic resumes when congestion alleviates. This option is valid only when traffic shaping is enabled.
- Throttle Then Shutdown - first queues traffic when congestion occurs, and then terminates the VC if throttling does not alleviate congestion. This option is valid only when traffic shaping is enabled.

Instructions: Choose a setting appropriate to your network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.33

Parameter: **Compression Control**

Path: Configuration Manager > Protocols > Frame Relay > Services > PVCs

Default: Enable

Options: Enable | Disable

Function: Enables or disables data compression for this service record.

Instructions: To use data compression for this service record, accept the default, Enable. Otherwise, select Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.29

Optional Algorithm Parameter for Each Multiline Configuration

The Services Multiline With window (Figure A-8) contains the Multiline Algorithm to Choose Line parameter.

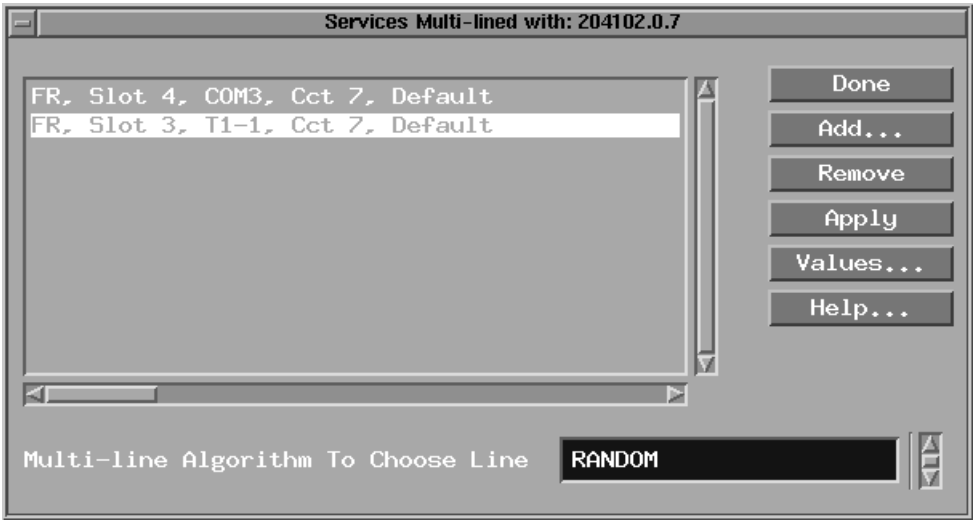

Figure A-8. Services Multiline With Window

To access the Services Multiline With window:

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on the **Multiline** button.	The Services Multi-line with window opens.

This window lets you:

- Specify how a multiline circuit distributes traffic by setting the Multiline Algorithm to Choose Line parameter.
- Add multiline services to a circuit.

  Click on **Add** to open the Add Multiline Services window (Figure A-9). Next, click on a circuit entry and click on **Select**. When you do this, the circuit entry moves from the Add Multiline Services window to the Services Multiline With window, indicating that it has been added to the multiline circuit. The Add Multiline Services window closes.

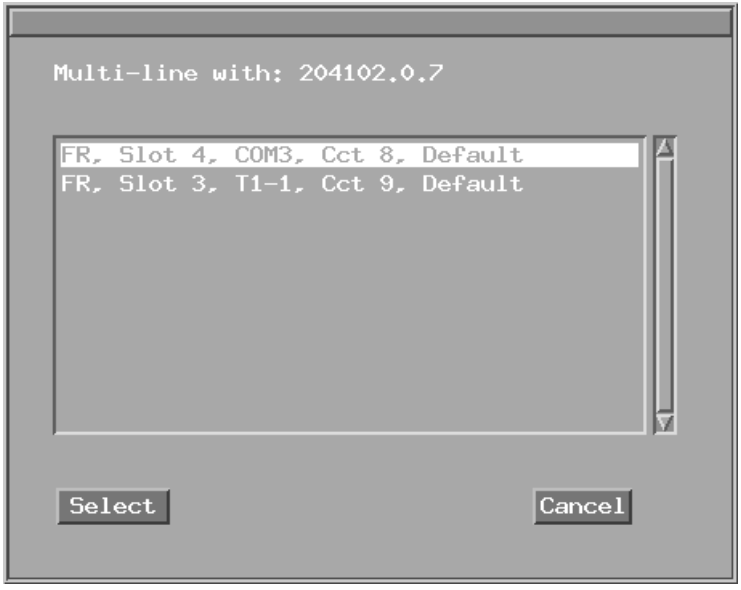

Figure A-9. Add Multiline Services Window

Parameter: **Multiline Algorithm to Choose Line**

Path: Configuration Manager > Protocols > Frame Relay > Services > Multiline

Default: None

Options: Random | Address Based

Function: Specifies how the multiline circuit distributes traffic over its data paths.

Instructions: To send data alternately over the two paths, select Random. This method ensures even distribution among the lines, but the packets arrive out of sequence. If the traffic between the same source and destination address pair is always going over the same data path, select Address Based. This method ensures the data arrives in sequence.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.1.1.23

SVC Service Record Parameters

The following topics describe SVC service record parameters.:

Topic	Page
SVC Service List Parameters	A-34
SVC Options Parameters	A-40
SVC Options List for Service Parameters	A-43

SVC Service List Parameters

You can edit SVC Service List parameters in the Frame Relay Service List window (Figure A-10). These parameters apply to all of the SVCs on the service record, unless you configure SVCs individually with SVC Options parameters.

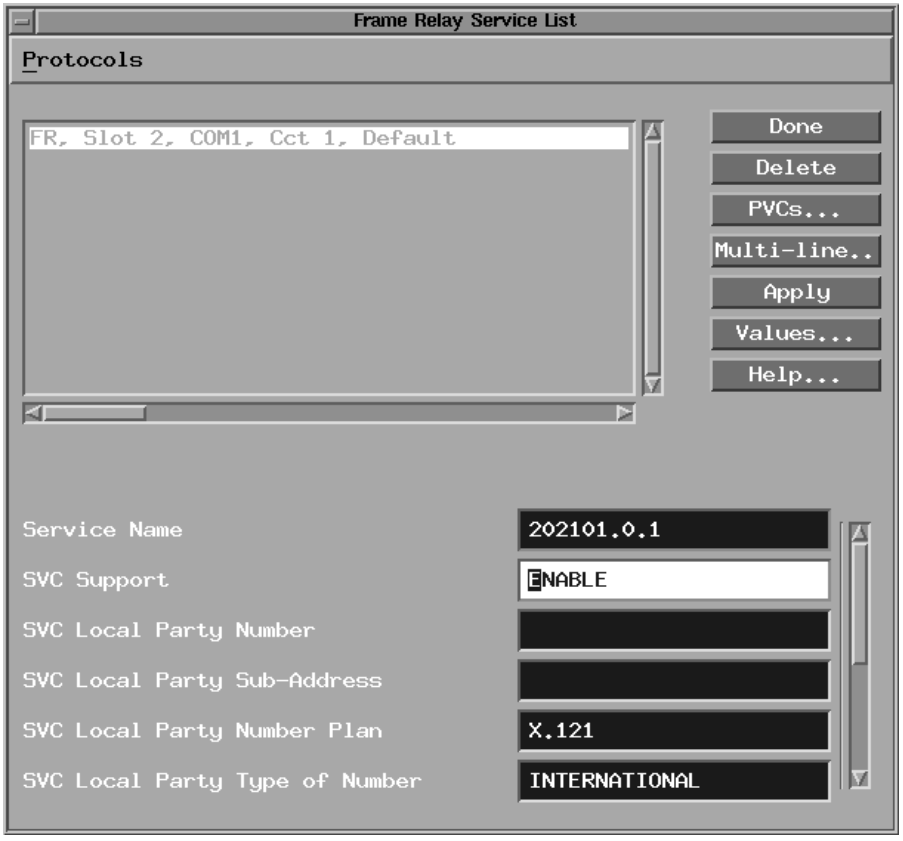

Figure A-10. Frame Relay Service List Window (for SVCs)

To access the Frame Relay Service List window:

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.

Note: You do not have access to the SVC parameters until you set the SVC Support parameter to Enable.

Parameter: Service Name

Path: Configuration Manager > Protocols > Frame Relay > Services
Default: None
Options: <*line number*>.0.<*circuit number*>
Function: Identifies the service record.
Instructions: Site Manager assigns a unique name in the format given to each service record. There is no need to change this value.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.5.1.7

Parameter: SVC Support

Path: Configuration Manager > Protocols > Frame Relay > Services
Default: Disable
Options: Enable | Disable
Function: Enables or disables support for SVCs on this interface.
Instructions: If you do not want to support SVCs on this interface, accept the default, Disable. If you do want to configure SVCs, choose Enable.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.5.1.17

Parameter: SVC Local Party Number

Path: Configuration Manager > Protocols > Frame Relay > Services
Default: None
Options: Any display string.
Function: The outbound calling part number, which is also the inbound called party number.
Instructions: Enter the number.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.5.1.18

Parameter: **SVC Local Party Sub-Address**

Path: Configuration Manager > Protocols > Frame Relay > Services
Default: None
Options: Any display string
Function: The outbound calling party sub-address, which is also the inbound called party sub-address.
Instructions: Enter the number.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.5.1.19

Parameter: **SVC Local Party Number Plan**

Path: Configuration Manager > Protocols > Frame Relay > Services
Default: X.121
Options: E.164 | X.121
Function: Specifies whether this SVC uses the E.164 or X.121 number plan for addresses.
Instructions: Choose the numbering plan that applies to your network.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.5.1.20

Parameter: **SVC Local Party Type of Number**

Path: Configuration Manager > Protocols > Frame Relay > Services
Default: International
Options: Unknown | International
Function: Specifies the type of number the local caller uses.
Instructions: To allow the caller to use an international type number, accept the default, International. Otherwise, choose Unknown.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.5.1.21

Parameter: SVC Call Block

Path: Configuration Manager > Protocols > Frame Relay > Services
Default: None
Options: None │ Inbound │ Outbound │ All
Function: Allows you to block certain types of calls on the SVC.
Instructions: Choose the type of call blocking you want this SVC to use.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.5.1.22

Parameter: SVC InScreening Disable

Path: Configuration Manager > Protocols > Frame Relay > Services
Default: Disable
Options: Enable | Disable
Function: Allows you to screen incoming calls on this SVC.
Instructions: If you do not want to screen incoming calls, accept the default, Disable. To screen calls, choose Enable.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.5.1.23

Parameter: SVC InScreening Usage

Path: Configuration Manager > Protocols > Frame Relay > Services
Default: Include
Options: Include | Exclude
Function: Enables you to allow or disallow calls from numbers in associated SVC option records.
Instructions: To allow these calls, accept the default, Include. Choose Exclude to disallow them.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.5.1.24

Parameter: SVC Inactivity Timer

Path: Configuration Manager > Protocols > Frame Relay > Services

Default: 60

Options: 0 to 2147483647 seconds

Function: Specifies the amount of time, in seconds, before the SVC terminates because no data has travelled over the circuit in the direction you specify in the Inactivity Mode parameter.

Instructions: If you want to set the timer to one minute, accept the default. Otherwise, specify another value within the allowable range.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.5.1.25

Parameter: SVC Inactivity Mode

Path: Configuration Manager > Protocols > Frame Relay > Services

Default: Both Directions

Options: Both Directions | Transmit Only | Receive Only | Either Direction

Function: Specifies the direction of traffic the Inactivity Timer monitors in determining whether to keep an SVC up or to terminate it.

- Transmit Only: the transmit timer expires.
- Receive Only: the receive timer expires.
- Both Directions: both the transmit AND the receive timers expire.
- Either Direction: either the transmit OR the receive timer expires.

Instructions: To monitor in both directions, accept the default. Otherwise, choose one of the other options.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.5.1.26

SVC Options Parameters

You can edit SVC Options parameters in the Frame Relay SVC Options Add window (Figure A-11).

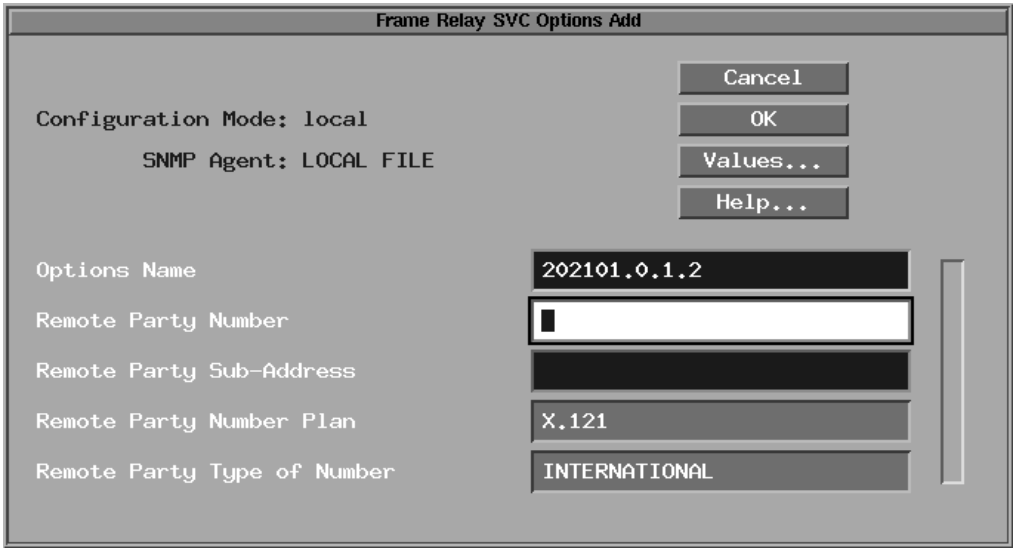

Figure A-11. Frame Relay SVC Options Add Window

To access the Frame Relay SVC Options window:

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on **SVCs.**	The Frame Relay Options List for Service window opens.
5. Click on **Add.**	The Frame Relay SVC Options Add window opens.

Parameter: Options Name

Path: Configuration Manager > Protocols > Frame Relay > Services > SVCs > Add

Default: None

Options: <*line number*>.0.<*circuit number*>

Function: Identifies the options record.

Instructions: Site Manager assigns a unique name in the format given. There is no need to change this value.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.34

Parameter: Remote Party Number

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > Services > Frame Relay Service List window > SVCs > Add

Default: None

Options: Any display string.

Function: Specifies the outbound called party number, which is also the inbound calling party number.

Instructions: Enter the number.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.7

Parameter: Remote Party Sub-Address

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > Services > Frame Relay Service List window > SVCs > Add

Default: None

Options: Any display string.

Function: The outbound called party sub-address, which is also the inbound calling party sub-address.

Instructions: Enter the number.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.8

Parameter: Remote Party Number Plan

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > Services > Frame Relay Service List window > SVCs > Add

Default: X.121

Options: E.164 | X.121

Function: Specifies whether the remote SVC uses the E.164 or X.121 number plan for addresses.

Instructions: Choose the numbering plan that applies to your network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.9

Parameter: Remote Party Type of Number

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > Services > Frame Relay Service List window > SVCs > Add

Default: International

Options: Unknown | International

Function: Specifies the type of number the remote caller uses.

Instructions: If the caller uses an international type number, accept the default, International. Otherwise, choose Unknown.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.10

SVC Options List for Service Parameters

When you have finished editing the Options parameters in the Options Add window, you can return to the Options List for Service window to edit the remaining options parameters for this SVC.

To access the Frame Relay Options List for Service window:

Path to Frame Relay Options List for Service Window	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on **SVCs**	The Frame Relay Options List for Service window opens.

Parameter: SVC Control

Path: Configuration Manager > Protocols > Frame Relay > Services > SVCs
Default: Enable
Options: Enable │ Disable
Function: Enables or disables SVC options record for this interface.
Instructions: Accept the default to enable the options record.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.2

Parameter: Broadcast Control

Path: Configuration Manager > Protocols > Frame Relay > Services > SVCs
Default: Enable
Options: Enable | Disable
Function: Specifies whether the router includes this interface in outbound broadcasts.
Instructions: If you want this SVC to receive outbound broadcasts, accept the default, Enable. Otherwise, choose Disable.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.11

Parameter: Inactivity Timer

Path: Configuration Manager > Protocols > Frame Relay > Services > SVCs
Default: 60
Options: 0 to 2147483647 seconds
Function: Amount of time, in seconds, before the SVC terminates because no data has travelled over the circuit in the direction you specify in the Inactivity Timer Mode parameter.
Instructions: Accept the default, or set to a value appropriate for your network.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.12

Parameter: Inactivity Timer Mode

Path: Configuration Manager > Protocols > Frame Relay > Services > SVCs
Default: Transmit Only
Options: Transmit Only | Receive Only | Both Directions | Either Direction
Function: Determines the kind of inactivity the Inactivity Timer parameter monitors.

- Transmit Only: the transmit timer expires.
- Receive Only: the receive timer expires.
- Both Directions: both the transmit AND the receive timers expire.
- Either Direction: either the transmit OR the receive timer expires.

Instructions: Accept the default, or choose another timer mode appropriate to your network.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.13

Parameter: X.213 Data Priority

Path: Configuration Manager > Protocols > Frame Relay > Services > SVCs

Default: 15

Options: 0 to 15

Function: Sets the priority of data on the network connection as defined in ITU-T Q.933 and X.213. This is a value the router requests; it is not guaranteed. A value of 0 is the lowest priority, with 14 as the highest. A value of 15 means unspecified.

Instructions: If your network supports X.213 prioritization, you should assign a value. You should accept the default if the network does not support X.213 prioritization, unless the network is able to accept pieces of signaling information that it does not recognize.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.14

Parameter: X.213 Data LQA Priority

Path: Configuration Manager > Protocols > Frame Relay > Services > SVCs

Default: 15

Options: 0 to 15

Function: Sets the lowest acceptable priority of data on a connection. A value of 0 is the lowest priority, with 14 as the highest. A value of 15 means unspecified.

Instructions: If your network supports X.213 prioritization, you should assign a value. You should accept the default if the network does not support X.213 prioritization, unless the network is able to accept pieces of signaling information that it does not recognize.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.15

Parameter: X.213 Gain Priority

Path: Configuration Manager > Protocols > Frame Relay > Services > SVCs

Default: 15

Options: 0 to 15

Function: Sets the priority of data required to add a connection. This is a value that the router requests; it is not guaranteed. A value of 0 is the lowest priority, with 14 as the highest. A value of 15 means unspecified.

Instructions: If your network supports X.213 prioritization, you should assign a value. You should accept the default if the network does not support X.213 prioritization, unless the network is able to accept pieces of signaling information that it does not recognize.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.16

Parameter: X.213 Gain LQA Priority

Path: Configuration Manager > Protocols > Frame Relay > Services > SVCs

Default: 15

Options: 0 to 15

Function: Sets the lowest acceptable priority of data to add a connection. This is a value below which the router will not create the SVC. A value of 0 is the lowest priority, with 14 as the highest. A value of 15 means unspecified.

Instructions: If your network supports X.213 prioritization, you should assign a value. You should accept the default if the network does not support X.213 prioritization, unless the network is able to accept pieces of signaling information that it does not recognize.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.17

Parameter: X.213 Keep Priority

Path:	Configuration Manager > Protocols > Frame Relay > Services > SVCs
Default:	15
Options:	0 to 15
Function:	Sets the priority of data required to maintain a connection. This is a value that the router requests; it is not guaranteed. A value of 0 is the lowest priority, with 14 as the highest. A value of 15 means unspecified.
Instructions:	If your network supports X.213 prioritization, you should assign a value. You should accept the default if the network does not support X.213 prioritization, unless the network is able to accept pieces of signaling information that it does not recognize.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.9.10.1.18

Parameter: X.213 Keep LQA Priority

Path:	Configuration Manager > Protocols > Frame Relay > Services > SVCs
Default:	15
Options:	0 to 15
Function:	Sets the lowest acceptable priority of data required to maintain a connection. This is a value below which the router will disconnect the SVC.
Instructions:	If your network supports X.213 prioritization, you should assign a value. You should accept the default if the network does not support X.213 prioritization, unless the network is able to accept pieces of signaling information that it does not recognize.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.9.10.1.19

Parameter: LL Core Out Throughput

Path: Configuration Manager > Protocols > Frame Relay > Services > SVCs
Default: 0
Options: 0 to 21447463647 b/s
Function: Specifies the requested outgoing throughput (b/s) when no congestion is occurring. To enable traffic shaping, the throughput parameters and the burst parameters must be set to values greater than zero.
Instructions: Choose a value appropriate to your network.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.20

Parameter: LL Core In Throughput

Path: Configuration Manager > Protocols > Frame Relay > Services > SVCs
Default: 0
Options: 0 to 21447463647 b/s
Function: Specifies the requested incoming throughput (kbits/second) when no congestion is occurring. To enable traffic shaping, the throughput parameters and the burst parameters must be set to values greater than zero.
Instructions: Choose a value appropriate to your network.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.21

Parameter: LL Core Min Out Throughput

Path: Configuration Manager > Protocols > Frame Relay > Services > SVCs
Default: 0
Options: 0 to 21447463647 b/s
Function: Specifies the minimum acceptable outgoing throughput. To enable traffic shaping, the throughput parameters and the burst parameters must be set to values greater than zero.
Instructions: Choose a value appropriate to your network.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.22

Parameter: LL Core Min In Throughput

Path: Configuration Manager > Protocols > Frame Relay > Services > SVCs

Default: 0

Options: 0 to 21447463647 b/s

Function: Specifies the minimum acceptable incoming throughput. To enable traffic shaping, the throughput parameters and the burst parameters must be set to values greater than zero.

Instructions: Choose a value appropriate to your network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.23

Parameter: LL Core Out Committed Burst

Path: Configuration Manager > Protocols > Frame Relay > Services > SVCs

Default: 0

Options: 0 to 21447463647 b/s

Function: Specifies the outgoing committed burst size. This is the maximum number of bits that a VC can transmit during the VC's burst period (Tc) when congestion is occurring. To enable traffic shaping, this parameter and the Throughput parameter (CIR) must both be greater than zero. The Core Out Committed Burst (Bc) value should be lower than the Core Out Throughput value.

Instructions: Choose a value appropriate to your network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.24

Parameter: LL Core In Committed Burst

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > Services > Frame Relay Service List window > SVCs > Add

Default: 0

Options: 0 to 21447463647 b/s

Function: Specifies the incoming committed burst size. This is the maximum number of bits that a VC can receive during the VC's burst period (Tc) when congestion is occurring. To enable traffic shaping, the Burst parameters and the Throughput parameters (CIR) must both be greater than zero. The Core In Committed Burst (Bc) value should be lower than the Core In Throughput value.

Instructions: Choose a value appropriate to your network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.25

Parameter: LL Core Out Excess Burst

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > Services > Frame Relay Service List window > SVCs > Add

Default: 0

Options: 0 to 21447463647 b/s

Function: Specifies the outgoing excess burst size. This value is added to the Core Out Committed Burst value to determine the maximum number of bits that may be transmitted during the VC's burst period when there is no congestion. The Core Out Excess Burst plus the Core Out Committed Burst must be less than or equal to the line speed.

Instructions: Choose a value appropriate to your network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.26

Parameter: LL Core In Excess Burst

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > Services > Frame Relay Service List window > SVCs > Add

Default: 0

Options: 0 to 21447463647 b/s

Function: Specifies the incoming excess burst size. This value is added to the Core In Committed Burst value to determine the maximum number of bits that may be transmitted during the VC's burst period when there is no congestion. The Core In Excess Burst plus the Core In Committed Burst must be less than or equal to the line speed.

Instructions: Choose a value appropriate to your network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.27

Parameter: Congestion Disable

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > Services > Frame Relay Service List window > SVCs > Add

Default: Inherit

Options: Enable | Disable | Inherit

Function: Specifies whether and how this SVC will use congestion control.

- Inherit means that this SVC uses the value in the interface Congestion Control parameter.
- Enable activates congestion control for this SVC regardless of the setting in the Interface parameter. If you enable congestion control, the router drops all outbound traffic from this SVC while congestion is occurring.
- Disable means that the SVC will not use congestion control.

Instructions: Accept the default, or choose another value appropriate to your network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.28

Parameter: Congestion Timer

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > Services > Frame Relay Service List window > SVCs > Add

Default: 1

Options: 0.5 to 5 seconds, in 0.5-second intervals

Function: Specifies the length of time, in seconds, during which the router counts congestion notifications. If the router receives the number of congestion notifications set by the congestion counter parameter, the router stops transmitting data. The router resumes transmission once it stops receiving congestion notifications.

Instructions: Set the length of time the router should count congestion notifications from the network. If you set this parameter for a long time period, the router may be less likely to stop transmission for an intermittent congestion condition. However, the router may be slow to detect congestion, resulting in long transmission delays once the congestion has cleared.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.29

Parameter: Congestion Counter

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > Services > Frame Relay Service List window > SVCs > Add

Default: 20

Options: 1 to 500 notifications

Function: Indicates the maximum number of congestion notifications that the router can receive during the congestion timer period before it stops transmitting. If the router reaches the value set by this parameter, it determines the line is congested and stops transmitting.

Instructions: Set the congestion count. The smaller the number, the more quickly the router detects congestion and stops transmitting. The value of this parameter applies to all VCs that you do not individually configure.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.30

Parameter: Congestion Method

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > Services > Frame Relay Service List window > SVCs > Add

Default: Inherit

Options: Shutdown │ Throttle │ Throttle Then Shutdown │ Inherit

Function: Specifies the method of congestion control:

- Shutdown terminates the VC when congestion occurs.
- Throttle queues traffic when congestion occurs; traffic resumes when congestion alleviates. This option is valid only when traffic shaping is enabled.
- Throttle Then Shutdown first queues traffic when congestion occurs, and then terminates the VC if throttling does not alleviate congestion. This option is valid only when traffic shaping is enabled.
- Inherit uses the value in the Interface Congestion Method parameter.

Instructions: Choose a setting appropriate to your network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.31

Parameter: Traffic Shaping Disable

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > Services > Frame Relay Service List window > SVCs > Add

Default: Disable

Options: Enable │ Disable

Function: Enables or disables traffic shaping on this SVC.

Instructions:

- If you do not want to use traffic shaping on this SVC, accept the default, Disable, and do not set the LL Core parameters.
- To use traffic shaping and accept the QoS the network provides, set this parameter to Enable, and do not configure the LL Core parameters.
- To use traffic shaping, and negotiate QoS with the network, set this parameter to Enable, and also set the LL Core parameters.
- To prevent the router from enforcing the CIR, set this parameter to Disable, and also set the LL Core parameters.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.32

Parameter: WCP Enable

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > Services > Frame Relay Service List window > SVCs > Add

Default: Enable

Options: Enable | Disable

Function: Enables or disables compression services for this SVC.

Instructions: Accept the default, Enable, to use compression on this SVC. Choose Disable to disable but not delete compression services.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.33

WHERE DOES THIS PARAMETER GO?

Parameter: XOFF

Path: Configuration Manager > Edit Circuit> Interfaces > Interfaces

Default: Enable

Options: Enable | Disable

Function: Enables or disables frame relay service on this port.

Instructions: To disable ?? on this interface without deleting it, set to Disable. To reenable ??, if you previously disabled it, set to Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1. ??

Appendix B
RIP Management for Frame Relay SVCs

IP and IPX use RIP to inform network entities of routing topology changes. Both IP and IPX allow various controls over the frequency and destination of these packets. Because RIP packets can affect whether and how the router establishes and disconnects frame relay SVCs, these controls extend to frame relay SVCs. Table B-1 lists the IP, IPX, and frame relay configuration attributes that affect frame relay SVCs, and how they interact.

For more information about configuring RIP see *Configuring IP Services* and *Configuring IPX Services*.

Table B-1. RIP Parameters

IP or IPX RIP Enable	IP or IPX RIP Frame Relay SVC Broadcast Enable	Frame Relay SVC Inactivity Timer Mode	Inactivity Timer, RIP Timer	RIP Timer Functionality	Inactivity Timer Functionality
Enabled	Enabled	Both Directions	Inactivity > RIP	When the RIP timer expires: • RIP packets will be sent over connected SVCs. • Any SVCs configured as adjacent hosts that are not connected will be connected in order to send RIP packets.	RIP packets will refresh the transmit inactivity timer, any connected SVCs will never disconnect due to inactivity.
Enabled	Disabled	Both Directions	Inactivity > RIP	When the RIP timer expires: • RIP packets will be sent over connected SVCs. • Any SVCs configured as adjacent hosts that are not connected will remain disconnected. SVCs will not be connected in order to send RIP packets.	RIP packets will refresh the transmit inactivity timer, any connected SVCs will never disconnect due to inactivity.

Table B-1. RIP Parameters *(continued)*

IP or IPX RIP Enable	IP or IPX RIP Frame Relay SVC Broadcast Enable	Frame Relay SVC Inactivity Timer Mode	Inactivity Timer, RIP Timer	RIP Timer Functionality	Inactivity Timer Functionality
Enabled	Enabled	Both Directions	Inactivity < RIP	When the RIP timer expires: • RIP packets will be sent over connected SVCs. • Any SVCs configured as adjacent hosts that are not connected will be connected in order to send RIP packets.	If no non RIP packets are transmitted AND no packets are received within the inactivity timer interval, the SVC will be disconnected.
Enabled	Disabled	Both Directions	Inactivity < RIP	When the RIP timer expires: • RIP packets will be sent over connected SVCs. • Any SVCs configured as adjacent hosts that are not connected will remain disconnected. SVCs will not be connected in order to send RIP packets.	If no non RIP packets are transmitted AND no packets are received within the inactivity timer interval, the SVC will be disconnected.
Disabled	Enabled or Disabled	Both Directions	RIP timer not applicable, RIP is disabled.	Not applicable, RIP is disabled.	If no packets are transmitted AND no packets are received within the inactivity timer interval, the SVC will be disconnected.

Table B-1. RIP Parameters *(continued)*

IP or IPX RIP Enable	IP or IPX RIP Frame Relay SVC Broadcast Enable	Frame Relay SVC Inactivity Timer Mode	Inactivity Timer, RIP Timer	RIP Timer Functionality	Inactivity Timer Functionality
Enabled	Enabled	Either Direction	Inactivity > RIP	When the RIP timer expires: • RIP packets will be sent over connected SVCs. • Any SVCs configured as adjacent hosts that are not connected will be connected in order to send RIP packets.	RIP packets will refresh the transmit inactivity timer. If no packets are received within the inactivity timer interval, the SVC will be disconnected.
Enabled	Disabled	Either Direction	Inactivity > RIP	When the RIP timer expires: • RIP packets will be sent over connected SVCs. • Any SVCs configured as adjacent hosts that are not connected will remain disconnected. SVCs will not be connected in order to send RIP packets.	RIP packets will refresh the transmit inactivity timer. If no packets are received within the inactivity timer interval, the SVC will be disconnected.
Enabled	Enabled	Either Direction	Inactivity < RIP	When the RIP timer expires: • RIP packets will be sent over connected SVCs. • Any SVCs configured as adjacent hosts that are not connected will be connected in order to send RIP packets.	If no non RIP packets are transmitted OR if no packets are received within the inactivity timer interval, the SVC will be disconnected.

Table B-1. RIP Parameters *(continued)*

IP or IPX RIP Enable	IP or IPX RIP Frame Relay SVC Broadcast Enable	Frame Relay SVC Inactivity Timer Mode	Inactivity Timer, RIP Timer	RIP Timer Functionality	Inactivity Timer Functionality
Enabled	Disabled	Either Direction	Inactivity < RIP	When the RIP timer expires: • RIP packets will be sent over connected SVCs. • Any SVCs configured as adjacent hosts that are not connected will remain disconnected. SVCs will not be connected in order to send RIP packets.	If no non RIP packets are transmitted OR if no packets are received within the inactivity timer interval, the SVC will be disconnected.
Disabled	Enabled or Disabled	Either Direction	RIP timer not applicable, RIP is disabled.	Not applicable, RIP is disabled.	If no packets are transmitted OR no packets are received within the inactivity timer interval, the SVC will be disconnected.
Enabled	Enabled	Transmit	Inactivity > RIP	When the RIP timer expires: • RIP packets will be sent over connected SVCs. • Any SVCs configured as adjacent hosts that are not connected will be connected in order to send RIP packets.	RIP packets will refresh the transmit inactivity timer, any connected SVCs will never disconnect due to inactivity.

Table B-1. RIP Parameters *(continued)*

IP or IPX RIP Enable	IP or IPX RIP Frame Relay SVC Broadcast Enable	Frame Relay SVC Inactivity Timer Mode	Inactivity Timer, RIP Timer	RIP Timer Functionality	Inactivity Timer Functionality
Enabled	Disabled	Transmit	Inactivity > RIP	When the RIP timer expires: • RIP packets will be sent over connected SVCs. • Any SVCs configured as adjacent hosts that are not connected will remain disconnected. SVCs will not be connected in order to send RIP packets.	RIP packets will refresh the transmit inactivity timer, any connected SVCs will never disconnect due to inactivity.
Enabled	Enabled	Transmit	Inactivity < RIP	When the RIP timer expires: • RIP packets will be sent over connected SVCs. • Any SVCs configured as adjacent hosts that are not connected will be connected in order to send RIP packets.	If no non RIP packets are transmitted within the inactivity timer interval, the SVC will be disconnected.
Enabled	Disabled	Transmit	Inactivity < RIP	When the RIP timer expires: • RIP packets will be sent over connected SVCs. • Any SVCs configured as adjacent hosts that are not connected will remain disconnected. SVCs will not be connected in order to send RIP packets.	If no non RIP packets are transmitted within the inactivity timer interval, the SVC will be disconnected.

Table B-1. RIP Parameters *(continued)*

IP or IPX RIP Enable	IP or IPX RIP Frame Relay SVC Broadcast Enable	Frame Relay SVC Inactivity Timer Mode	Inactivity Timer, RIP Timer	RIP Timer Functionality	Inactivity Timer Functionality
Disabled	Enabled or Disabled	Transmit	RIP timer not applicable, RIP is disabled.	Not applicable, RIP is disabled.	If no packets are transmitted within the inactivity timer interval, the SVC will be disconnected.
Enabled	Enabled	Receive	Inactivity > RIP	When the RIP timer expires: • RIP packets will be sent over connected SVCs. • Any SVCs configured as adjacent hosts that are not connected will be connected in order to send RIP packets.	If no packets are received within the inactivity timer interval, the SVC will be disconnected.
Enabled	Disabled	Receive	Inactivity > RIP	When the RIP timer expires: • RIP packets will be sent over connected SVCs. • Any SVCs configured as adjacent hosts that are not connected will remain disconnected. SVCs will not be connected in order to send RIP packets.	If no packets are received within the inactivity timer interval, the SVC will be disconnected.

Table B-1. RIP Parameters *(continued)*

IP or IPX RIP Enable	IP or IPX RIP Frame Relay SVC Broadcast Enable	Frame Relay SVC Inactivity Timer Mode	Inactivity Timer, RIP Timer	RIP Timer Functionality	Inactivity Timer Functionality
Enabled	Enabled	Receive	Inactivity < RIP	When the RIP timer expires: • RIP packets will be sent over connected SVCs. • Any SVCs configured as adjacent hosts that are not connected will be connected in order to send RIP packets.	If no packets are received within the inactivity timer interval, the SVC will be disconnected.
Enabled	Disabled	Receive	Inactivity < RIP	When the RIP timer expires: • RIP packets will be sent over connected SVCs. • Any SVCs configured as adjacent hosts that are not connected will remain disconnected. SVCs will not be connected in order to send RIP packets.	If no packets are received within the inactivity timer interval, the SVC will be disconnected.
Disabled	Enabled or Disabled	Receive	RIP timer not applicable, RIP is disabled.	Not applicable, RIP is disabled.	If no packets are received within the inactivity timer interval, the SVC will be disconnected.

Appendix C
Monitoring Frame Relay Using BCC show Commands

Use the BCC **show frame-relay** command to display configuration and statistical information about frame relay services. For information about **show** command syntax, see *Using the Bay Command Console.*

Online Help for show Commands

You can display a list of available command options by entering **show** *<option>* without additional options or with a question mark as an option. For example, entering **show frame-relay ?** at the BCC prompt displays the list of all **show frame-relay** keyword (subcommand) options.

Commands for Frame Relay

The **show frame-relay** *<container>* command displays information about the router's frame-relay configuration.

Table C-1 lists all **show frame-relay** commands. The filter flag and filter arguments are options that you can use with each keyword (also called subcommand).

Table C-1. Frame Relay Show Commands

<container>	**<keyword>**	**<arguments>**	**<filter_flags>**	**<filter_arguments>**
frame-relay	summary	<none>	-state -type	*<interface_name>* {backup | normal | primary | demand}
frame-relay	vcs	<none>	-dlci -interface -service -type -state	*<dlci>* *<name>* *<name>* {pvc | dynamic-pvc | svc} {active | inactive | xoff | control | starting}
frame-relay	services	<none>	-interface -service	*<name>* *<name>*
frame-relay	shaping	<none>	-dlci -interface -service	*<dlci>* *<name>* *<name>*
frame-relay	congestion	<none>	-dlci -interface -service -state	*<dlci>* *<name>* *<name>* {forwarding | throttling | shutdown}
frame-relay	svcs	{calls | priority | shaping}	-dlci -interface -service	*<dlci>* *<name>* *<name>*
frame-relay	multiline	{services | pvcs}	-dlci -name	*<dlci>* *<multiline>*
frame-relay stats	vcs	*<none>*	-dlci -interface -service -type	*<dlci>* *<name>* *<name>* {pvc | dynamic-pvc | svc}

(continued)

Table C-1. Frame Relay Show Commands *(continued)*

<container>	<keyword>	<arguments>	<filter_flags>	<filter_arguments>
frame-relay stats	shaping	{low | normal | high | sum}	-dlci -interface -service	*<dlci>* *<name>* *<name>*
frame-relay stats	dlcmi	*<none>*	-interface	*<name>*
frame-relay stats	lapf	{receive | transmit | error | traffic}	-interface	*<name>*
frame-relay stats	signalling	{receive | transmit}	-interface	*<name>*
frame-relay stats	error	*<none>*	-interface	*<name>*

show frame-relay

The **show frame-relay** *<option>* commands display configuration, state, and statistical information about frame relay services.

The **show frame-relay** command supports the following subcommand options:

summary [-state {enabled | disabled | error}] [-type {backup | normal | primary | demand}]	congestion [-dlci <dlci>] [interface <name>] [-service <name>] [-state {forwarding | throttling | shutdown}]
vcs [-dlci <dlci>] [-interface <name>] [-service <name>] [-type {pvc | dynamic-pvc | svc}] [-state {active | inactive | invalid | xoff | control | starting}]	svcs {calls | priority | shaping} [-dlci <dlci>] [-interface <name>] [-service <name>]
services [-interface <name>] [-service <name>]	multiline {services | pvcs} [-dlci <dlci>] [-name <multiline_name>]
services [-interface <name>] [-service <name>]	vcs [-dlci <dlci> [-interface <name>] [-service <name>] [-type {pvc | dynamic-pvc | svc}]
shaping [-dlci <dlci>] [-interface <name>] [-service <name>]	

summary [-state {enabled | disabled | error}] [-type {backup | normal | primary | demand}]

Displays general information about all frame relay interfaces. You can display the current operational status and interface type.

This command allows for the following command filters and filter arguments:

-state {enabled | disabled | error}	Displays information about the state of the frame relay interfaces: • *enabled* -- shows only frame relay interfaces that are enabled. • *disabled* -- shows only frame relay interfaces that are disabled. • *error* -- shows only frame relay interfaces that are not present or are in a fault state.
-type {backup | normal | primary | demand}	• *backup* – shows only frame relay interfaces used to back up another frame relay interface. • *normal* -- shows only frame relay interfaces that are not backup, primary, or demand frame relay interfaces. • *primary* -- shows only frame relay interfaces that have a backup frame relay interface assigned to them. • *demand* -- shows only frame relay interfaces that are dial-on-demand.

The output includes the following information:

Interface	The interface on which the frame relay circuit resides.
Circuit	Name of the main frame relay circuit associated with this interface.
Management Type	Type of Data Link Control Management Interface (DLCMI) configured for the interface, as follows: • *Annex A* - Management services as specified by CCITT Annex A. • *Annex D* - Management services as specified in Annex D to ANSI standard TI.617. • *Annex A Sw* - Management services for the DCE side of the connection (Annex A). • *Annex D Sw* - Management services for the DCE side of the connection (Annex D to TI.617). • *LMI* - Management services as specified by Revision 1 of the Local Management Interface standard. • *LMI Sw* - Management services for the DCE side of LMI. • *None* - No management interface between the router and the frame relay network.
Interface Type	Interface type: Normal (leased service with no backup service), Primary/Shared (the backup circuit uses the primary configuration), Primary/Secondary (the backup circuit uses its own configuration).
Status	State of the interface as follows: • *Fault* - Interface is not operating. • *Init* - Interface is initializing (has not yet started). • *NotPres* - Interface is not yet present. • *Running* - Interface is operating properly.
Faults	Number of times the interface has been in fault mode.
Number of VCs --Total	Total number of VCs configured on the interface.
Number of VCs --Active	Total number of VCs active on the interface.
Services	Total number of frame relay service records or circuits.

vcs [-dlci *<dlci>*] [-interface *<name>*] [-service *<name>*] [-type {pvc | dynamic-pvc | svc}] [-state {active | inactive | invalid | xoff | control | starting}]

Displays information about all those frame relay VCs with the specified DLCI. This command allows for the following command filters and filter arguments:

-dlci *<dlci>*	Displays only frame relay VCs with the specified DLCI.
-interface *<name>*	Displays only frame relay interfaces configured on the specified interface.
-service *<name>*	Displays only frame relay VCs on the specified service record.
-type {pvc | dynamic-pvc | svc}	Displays information about only those VCs of type: • *pvc* -- shows only frame relay VCs that are statically configured PVCs. • *dynamic-pvc* -- shows only frame relay VCs that are dynamically learned PVCs. • *svc* -- shows only frame relay VCs that are SVCs.
-state {active | inactive | invalid | xoff | control | starting}	Displays information about only those VCs in one of the following states: • *Invalid* -- VC is configured but the switch has not confirmed it. • *Active* -- VC is usable. • *Inactive* -- VC is configured but not active. • *xoff* -- VCs are XOFF'd. • *control* -- shows only control VCs • *starting* -- shows VCs that are starting

The output includes the following information:

Interface	The interface on which the frame relay circuit resides.
DLCI	Name of the virtual circuit associated with this interface.
State	State of the virtual circuit as follows: • *Invalid* -- Circuit is configured but the switch has not confirmed it. • *Active* -- Circuit is usable. • *Inactive* -- Circuit is configured but not active. • *xoff* -- Specifies whether the router ignores or observes the XOFF bit in LMI. • *control* -- Circuit is a control VC. • *starting* -- Circuit is a starting VC.
Type	Type of circuit configured on the interface: • *pvc* -- PVC was statically configured. • dynamic-pvc -- PVC was dynamically learned. • *svc* -- VC is an SVC.
Hybrid	Indicates that you can use the same PVC for both routing and bridging.
Service	The service name associated with this PVC.

services [-interface *<name>*] [-service *<name>*]

Displays general information about all frame relay services, including the number of VCs and SVC configurations. This command allows for the following command filters and filter arguments:

-interface *<name>*	Displays only frame relay services on the specified interface.
-service *<name>*	Displays only frame relay VCs on the specified service.

The output includes the following information:

Interface	The interface on which the frame relay circuit resides.
Service-Name	Identifies the unique name assigned to the service.
Total Number of VCs	Total number of VCs configured on this interface.
Number of VCs -- Static	Total number of static VCs configured on this interface.
Number of VCs -- Dynamic	Total number of PVCs dynamically learned.
Number of VCs -- SVCs	Total number of SVCs configured on this interface.
Number of VCs-- Active	Total number of VCs active on this interface.
Multiline	Specifies whether the service record is for multiline.

shaping [-dlci *<dlci>*] [-interface *<name>*] [-service *<name>*]

Displays information about the traffic shaping configuration of all frame relay VCs. This command allows for the following command filters and filter arguments:

-dlci *<dlci>*	Displays only frame relay VCs with the specified DLCI.
-interface *<name>*	Displays only frame relay VCs configured on the specified interface.
-service *<name>*	Displays only frame relay VCs on the specified service.

The output includes the following information:

Interface	The interface on which the frame relay circuit resides.
DLCI	Name of the VC associated with this circuit.
CIR	Committed information rate.
Committed Burst	The maximum number of bits that the router can transmit over a specified time interval ($B_{c)}$.
Excess Burst	The maximum number of extra bits the router attempts to send when there is no congestion ($B_{e)}$.
Config Mode	Indicates whether the circuit is configured to use traffic shaping.
Congestion State	Status of traffic; options are: • *forwarding* -- sending traffic at up to the maximum rate allowed on the PVC. • *congested* -- the PVC is not transmitting. • *throttling* -- the PVC is throttling back to the CIR rate.

congestion [-dlci *<dlci>*] [interface *<name>*] [-service *<name>*] [-state {forwarding | throttling | shutdown}]

Displays information about the congestion state and the configuration of frame relay VCs. This command allows for the following command filters and filter arguments:

-dlci *<dlci>*	Displays only frame relay VCs with the specified DLCI.
-interface *<name>*	Displays only frame relay VCs configured on the specified interface.
-service *<name>*	Displays only frame relay VCs on the specified service.
-state {**forwarding | throttling | shutdown**}	Displays information about VCs in the following states: • *forwarding* -- shows only frame relay VCs that are forwarding. • *throttling* -- shows only frame relay VCs that are throttling. • *shutdown* -- shows only frame relay VCs that are shut down.

The output contains the following information:

Interface	The interface on which the frame relay circuit resides.
DLCI	Name of the VC associated with this circuit.
Enable	Status of congestion control: Disabled, Enabled, or Inherit. Inherit indicates that the VC should use the parameters from the DLCMI record.
State	Status of traffic; options are • *forwarding* -- sending traffic at up to the maximum rate allowed on the PVC. • *congested* -- the PVC is not transmitting. • *throttling* -- the PVC is throttling back to the CIR rate.
Method	Identifies the congestion method: • *Shutdown* -- the VC terminates when congestion occurs. • *Throttle* -- the VC queues traffic when congestion occurs; traffic resumes when the congestion alleviates. • *Throttle then shutdown* -- first queues traffic when congestion occurs, and then terminates the VC if throttling does not alleviate congestion. • *Inherit* -- the VC uses the parameter from the DLCMI record.
Timer	Length of time in seconds during which the router counts congestion notifications.
Counter	Maximum number of congestion notifications that the router can receive during the timer period before it stops transmitting.
Received FECN	Number of outbound forward explicit congestion notifications.
Received BECN	Number of outbound backward explicit congestion notifications.

svcs {calls | priority | shaping} [-dlci *<dlci>*] [-interface *<name>*] [-service *<name>*]

Displays general information about all frame relay SVCs. You can display current operation status and SVC type.

svcs calls

Displays call information for active frame relay SVCs. This command allows for the following command filters and filter arguments:

-dlci *<dlci>*	Displays only frame relay SVCs with the specified DLCI.
-interface *<name>*	Displays only frame relay SVCs configured on the specified interface.
-service *<name>*	Displays only frame relay SVCs on the specified service.

The output contains the following information:

Interface	Interface on which the SVC resides.
DLCI	Name of the SVC associated with this circuit.
Direction	Direction of the call to the router: inbound or outbound.
Calling Number	Number the router is calling.
Called Number	Router being called.

svcs priority

Displays priority information for active frame SVCs. This command allows for the following command filter and filter arguments:

-dlci *<dlci>*	Displays only SVCs with the specified DLCI.
-interface *<name>*	Displays only SVCs configured on the specified interface.
-service *<name>*	Displays only SVCs on the specified service.

The output contains the following information:

Interface	Interface on which the SVC resides.
DLCI	Name of the SVC associated with this circuit.
Data Priority	Priority of data on the network connection. This is a value that the router requests; it is not guaranteed.
Gain Priority	Priority of data required to add a connection. This is a value that the route requests; it is not guaranteed.
Keep Priority	Priority of data required to maintain a connection. This is a value the router requests; it is not guaranteed.

svcs shaping

Displays shaping information for active SVCs. This command allows for the following command filter and filter arguments:

-dlci *<dlci>*	Displays only SVCs with the specified DLCI.
-interface *<name>*	Displays only SVCs configured on the specified interface.
-service *<name>*	Displays only SVCs on the specified service.

The output contains the following information:

Interface	Interface on which the SVC resides.
DLCI	Name of the SVC associated with this circuit.
CIR	Committed information rate, or throughput, indicates the number of bits per second a carrier guarantees the router can transmit over a specified time interval when there is no congestion.
Inbound Burst CIR	Number of requested incoming throughput (kbits/second) when no congestion is occurring.
Inbound Burst Committed	Number of bits that the router can receive over a specified time interval (B_c).
Inbound Burst Excess	Number of extra bits the router attempts to receive when there is no congestion (B_e).
Outbound Burst CIR	Requested outgoing throughput when no congestion is occurring.
Outbound Burst Committed	The number of bits that the router can send over a specified time interval ($B_{c)}$.
Outbound Burst Excess	The number of extra bits the router attempts to send when there is no congestion ($B_{e)}$.

multiline {services | pvcs} [-dlci *<dlci>*] [-name *<multiline_name>*]

Displays information about frame relay service information for multiline and shows PVCs that are priority information for active frame relay SVCs.

multiline services

Shows frame relay information for multiline.This command allows for the following command filters and filter arguments:

-dlci *<dlci>*	Displays only VCs with the specified DLCI.
-name *<multiline_name>*	Displays only multiline PVCs or services on the specified frame relay multiline.

The output contains the following information:

Multiline-Name	Name of the multiline circuit.
Interface	Interface on which the multiline circuit resides.
Service-Name	Service name associated with the multiline.
Number of VCs	Total number of VCs on the multiline.

multiline pvcs

Displays PVCs that are priority information for active frame relay SVCs. This command allows for the following command filters and filter arguments:

-dlci *<dlci>*	Displays only PVCs with the specified DLCI.
-name *<multiline_name>*	Displays only multiline PVCs or services on the specified frame relay multiline.

The output contains the following information:

Interface	Interface on which the frame relay SVC resides.
DLCI	Name of the SVC associated with this circuit.
Service-Name	Service name associated with the multiline.
Multiline-Name	Name of the multiline circuit.

show frame-relay stats

The **show frame-relay stats** *<option>* commands display statistical information about frame relay services.

The **show frame-relay stats** command supports the following subcommand options:

vcs [-dlci <dlci> [-interface <name>] [-service <name>] [-type {pvc | dynamic-pvc | svc}]	lapf {receive | transmit | error | traffic} [-interface <name>]
shaping {high | normal | low | sum} [-dlci <dlci>] [-interface <name>] [-service <name>]	signalling {receive | transmit} [-interface <name>]
dlcmi [-interface <name>]	errors [-interface <name>]

vcs [-dlci *<dlci>* [-interface *<name>*] [-service *<name>*] [-type {pvc | dynamic-pvc | svc}]

Displays inbound and outbound statistics for frame relay VCs. This command allows for the following command filters and filter arguments:

-dlci *<dlci>*	Displays only VCs with the specified DLCI.
-interface *<name>*	Displays only VCs configured on the specified interface.
-service *<name>*	Displays only VCs on the specified service.
-type {**pvc | dynamic-pvc | svc**}	Displays information about only the type of VC configured: • *pvc* -- shows only frame relay VCs that are statically configured PVCs. • *dynamic- pvc* -- shows only VCs that are dynamically learned PVCs. • *svc* -- shows only VCs that are SVCs.

The output contains the following information:

Interface	Interface on which the frame relay VC resides.
DLCI	Specifies the PVC identification number that the frame relay network uses to direct data.
Inbound Frames	Total number of frames that the interface received.
Inbound Drops	Total number of outbound frames dropped because the VC is inactive.
Outbound Frames	Total number of frames that the router sent out on this interface.
Outbound Discard	Total number of frames dropped because the VC is inactive.
FECN	Number of outbound forward explicit congestion notifications.
BECN	Number of outbound backward explicit congestion notifications.

shaping {high | normal | low | sum} [-dlci *<dlci>*] [-interface *<name>*] [-service *<name>*]

Displays high queue, normal queue, low queue, and summary traffic shaping statistics for frame relay VCs.

shaping high	Displays high queue outbound traffic shaping statistics for frame relay VCs.
shaping normal	Displays normal queue outbound traffic shaping statistics for frame relay VCs.
shaping low	Displays low queue outbound traffic shaping statistics for frame relay VCs.
shaping sum	Displays a summary of traffic shaping statistics for frame relay VCs.

This command allows for the following command filters and filter arguments:

-dlci *<dlci>*	Displays only VCs with the specified DLCI.
-interface *<name>*	Displays only VCs configured on the specified interface.
-service *<name>*	Displays only VCs on the specified service.

The output contains the following information:

Interface	Interface on which the frame relay VC resides.
DLCI	Name of the VC associated with this circuit.
Frames	Total number of frames that the router sends out this interface.
Inbound Drops	Total number of inbound frames dropped because the VC is inactive.
Frames Clipped from Queue	Number of high-, normal-, and low-priority clipped frames.
Maximum Frames in Queue	Maximum number of frames stored in the queue.
Queue Limit	Total number of buffers that the interface has to process frames.
Filter Dropped Frames	Total number of frames dropped because of congestion.
Large Frames	Number of large frames.

dlcmi [-interface *<name>*]

Displays inbound and outbound statistics for frame relay DLCMIs. This command allows for the following command filter and filter argument:

-interface *<name>*	Displays only DLCMI interfaces configured on the specified interface.

The output contains the following information:

Interface	Interface on which the DLCMI resides.
Maximum Number of VCs	Number of DLCMIs associated with this circuit.
Current Number of VCs	Total number of DLCMIs configured on the router.
Sequence Counter	Next send sequence counter for DLCMI messages sent by the station.
Received Sequence	Send sequence number received in the last DLCMI message.
Passive Sequence	This station's send sequence for answering the DLCMI message 'status enquiry.'
Passive Received	The sequence number received in the last DLCMI message 'status enquiry.'
Polls	Whether the station requests a full status report from the network or requests only a sequence number verification from the network.
Polls Missing	Number of missing status messages not received from a status enquiry.

lapf {receive | transmit | error | traffic} [-interface *<name>*]

Displays LAPF receive, transmit, traffic, and error statistics for frame relay interfaces.

lapf receive

Displays LAPF receive statistics for frame relay interfaces. This command allows for the following command filter and filter argument:

-interface *<name>*	Displays only frame relay interfaces configured on the specified interface.

The output contains the following information:

Interface	Interface on which the frame relay VC resides.
Window	Number of outstanding signalling messages allowed.
SABME	Set Asynchronous Balanced Mode Extended (SABME): command that initiates multiple frame operation.
UA	Unnumbered acknowledgment (UA) is a response sent by a station upon receipt of a SABME or DISC command.
DISC	Disconnect (DISC) is a command that initiates the release of multiple frame operation.
DM	Disconnect mode (DM) indicates the collision of commands and responses that prevent the initiation of multiple frame operations.
FRMR	Frame Reject (FRMR) indicates errors encountered that cannot be recovered by resending an information frame.
REJ	Reject (REJ) requests retransmission of information frames.
RNR	Receive not ready (RNR) indicates that the station is temporarily busy and not ready to receive information frames.
RR	Receive ready (RR) indicates that the station is ready to receive information frames.
XID	Exchange ID indicates the station's identification information.

lapf transmit

Displays LAPF transmit statistics for frame relay interfaces. This command allows for the following command filter and filter argument:

-interface *<name>*	Displays only frame relay VCs configured on the specified interface.

The output contains the following information:

Interface	Interface on which the frame relay VC resides.
Window	Number of outstanding signalling messages allowed.
SABME	Set Asynchronous Balanced Mode Extended (SABME): command that initiates multiple frame operation.
UA	Unnumbered acknowledgment (UA) is a response sent by a station upon receipt of a SABME or DISC command.
DISC	Disconnect (DISC) is a command that initiates the release of multiple frame operation.
DM	Disconnect mode (DM) indicates the collision of commands and responses that prevent the initiation of multiple frame operations.
FRMR	Frame reject (FRMR) indicates errors encountered that cannot be recovered by resending an information frame.
REJ	Reject (REJ) requests retransmission of information frames.
RNR	Receive not ready (RNR) indicates that the station is temporarily busy and not ready to receive information frames.
RR	Receive ready (RR) indicates that the station is ready to receive information frames.
XID	Exchange ID indicates the station's identification information.

lapf errors

Displays LAPF error statistics for frame relay interfaces. This command allows for the following command filter and filter argument:

-interface *<name>*	Displays only frame relay VCs configured on the specified interface.

The output contains the following information:

Interface	Interface on which the VC resides.
Retransmission (T200 Timeouts)	Indicates the length of time the router waits to receive an acknowledgment from the station.
Idle (T203 Timeouts)	Indicates the amount of time that the router allows with no data being transmitted.
Retransmission Limit Exceeded (N200 Violation)	Indicates that the router sends the SABME message based on the value contained in the N200 counter (wfLapfN200) without receiving a reply.
Frame Size Exceeded (N201 Violations)	Number of information frames whose length exceeds the maximum number of octets defined by N201 (wfLapfN201).

lapf traffic

Displays LAPF traffic statistics for frame relay interfaces. This command allows for the following command filter and filter argument:

-interface *<name>*	Displays only frame relay VCs configured on the specified interface.

The output contains the following information:

Interface	Interface on which the VC resides.
Unnumbered Frame Received	Number of frames received by LAPF in unnumbered format.
Numbered Frames Received	Number of frames received by LAPF.
Unnumbered Frames Sent	Number of frames sent by LAPF in unnumbered format.
Numbered Frames Sent	Number of frames sent by LAPF.

signalling {receive | transmit} [-interface *<name>*]

Displays receive and transmit statistics for frame relay interfaces.

signalling receive

Displays signalling receive statistics for frame relay interfaces. This command allows for the following command filter and filter argument:

-interface *<name>*	Displays only frame relay SVCs configured on the specified interface.

The output contains the following information:

Interface	Interface on which the SVC resides.
Setup	Indicates the number of seconds allowed from the time the router sends a setup message to the called subscriber and receives a connect or call proceeding message from the called subscriber.
Call Proceeding	Message sent by the called subscriber to the router or by the router to the calling subscriber to indicate the establishment of the requested call.
Connect	Message sent by the called subscriber to the router and by the router to the calling subscriber to indicate call acceptance by the called subscriber.
Disconnect	Message sent by the subscriber to request the router to clear an end-to-end connection or a message sent by the router to indicate that the end-to-end connection is cleared.
Release	Message sent by the user or router to indicate that the sender has disconnected the call.
Release Complete	Message sent by the subscriber or the router to indicate that the sender has released the call reference.
Status	Message sent by the subscriber or router in response to a status enquiry or to report error conditions.
Unnumbered Frames Sent	Number of unnumbered acknowledgment frames (UAs) sent over SVCs to a subscriber or router.
Status Enquiry	A message sent by the subscriber or router to solicit a status message.

signalling transmit

Displays signalling transmit statistics for frame relay interfaces. This command allows for the following command filter and filter argument:

-interface *<name>* Displays only SVCs configured on the specified interface.

The output contains the following information:

Interface	Interface on which the frame relay SVC resides.
Setup	Indicates the number of seconds allowed from the time the router sends a setup message to the called subscriber and receives a connect or call proceeding message from the called subscriber.
Call Proceeding	Indicates the number of seconds allowed from the time the router receives a call proceeding message to the time the router receives a connect or disconnect message.
Connect	Message sent by the called user to the network and by the network to the calling user to indicate call acceptance by the called user.
Disconnect	Indicates the number of seconds allowed from the time the router sends a disconnect message and receives a release message back.
Release	Indicates the number of seconds allowed for a call clearing initiated by the other end of the connection or when the disconnect timer expires.
Release Complete	Indicates that the network returns a release complete message to the subscriber in response to a release message sent from the subscriber.
Status	Message sent by the user or network in response to a status enquiry or to report error conditions.
Unnumbered Frames Sent	Number of unnumbered acknowledgment frames (UAs) sent over SVCs to a subscriber or router.
Status Enquiry	A message sent by the user or network to solicit a status message.

errors [-interface *<name>*]

Displays error statistics for frame relay interfaces. This command allows for the following command filter and filter argument:

-interface *<name>*	Displays only frame relay interfaces configured on the specified interface.

The output contains the following information:

Interface	Interface on which the frame relay SVC resides.
Last Error --Type	Type of the last error received.
Last Error -- Time	Time of the last error received.
Faults	Number of faults received.
Outbound Drops	Total number of outbound frames dropped because the SVC is inactive.
Inbound Discards	Total number of inbound frames discarded because they were deemed erroneous.

Index

A

access modes, 2-15
Action Initiate parameter, A-14
active state, 2-9
adding
  PVCs, 3-14
  PVCs to a service record, 2-15
  service records, 3-12
  SVCs, 3-41
adding service records, 3-35
Address Length parameter, A-6
Address parameter, A-6
address resolution, 2-18
address-based distribution for multiline, 2-36
adjacent hosts, 1-9
alerts
  fr, C-6
Annex A switch, 3-2
Annex D switch, 3-2

B

Bc
  configuring, 2-30
  description of, 2-24
Be
  description of, 2-24
BECN (backward explicit congestion notification)
  congestion control, 2-22
  definition of, 2-5
big pipe/little pipe, 2-20, 2-33
Broadcast Control parameter, A-44
buffers and traffic shaping, 2-32

C

call present state, 2-12
CIR
  definition of, 2-23
  enforcement, 2-24, 2-30
  maximum value, 2-24
  with a value of 0, 2-24
Circuit State Set parameter, A-27
Committed Burst parameter, A-28
committed burst rate. *See* Bc
committed information rate (CIR), 2-4
committed information rate. *See* CIR
Compression Control parameter, A-31
compression, of data, 2-21
congestion
  controlling, 3-58
congestion control
  configuring, 3-22
Congestion Control parameter, A-9, A-29
Congestion Counter parameter, A-10, A-30, A-52
Congestion Disable paramete, A-51
Congestion Method parameter, A-11, A-31, A-53
Congestion Timer parameter, A-10, A-30, A-52
congestion, description of, 2-22
customer support
  programs, xviii
  Technical Solutions Centers, xix
customizing frame relay, 3-1

D

data
  compression, 2-21
  encryption, 2-21
data compression, 3-70
  enabling, 3-32
  with traffic shaping, 2-30
data link control identifier (DLCI), 2-5
default service record, 2-14
deleting
  frame relay, 1-9, 3-74
  PVCs, 3-16
  service records, 3-38
dial backup, 2-38
dial-on-demand, 2-38
direct mode, 2-16
disabled circuits
  fr, C-7
disconnect indication state, 2-12
DLCI address length, selecting, 3-4
DLCI address type, selecting, 3-4
DLCI Number parameter, A-25
DLCMI (Data Link Control Management Interface)
  definition of, 2-7
  standards of, 2-7

E

editing
  congestion control parameters, 3-58
  LAPF parameters, 3-44
  signaling parameters, 3-50
  traffic shaping parameters, 3-65
Enable parameter (Interface), A-4
Enable parameter (SVC LAPF), A-13
enabled circuits
  fr, C-8
enabling frame relay, 1-1
encryption of data, 2-21
error threshold, 3-7
Error Threshold parameter, A-8
Excess Burst parameter, A-28
excess burst. *See* Be
exchange identification (XID) frames, 2-9

F

FECN (forward explicit congestion notification)
  congestion control, 2-22
  definition of, 2-5
FR PVC List for Service window, A-26
frame relay
  deleting from a router, 1-9
  overview, 2-2
  reference sources, 2-39
  starting, 1-1
Frame Relay Interface List Window for PVCs, A-2
Frame Relay PVC Add Window, A-24
Frame Relay Service List window, A-23
Frame Relay Signaling Parameters Window, A-17
Frame Relay SVC Options Add window, A-40
full enquiry interval, 3-7
Full Enquiry Interval parameter, A-7

G

group mode, 2-15
grouping service records for multiline, 3-34

H

header format
  2-byte, 2-6
  3- or 4-byte, 2-6
hybrid mode, 2-16
Hybrid Mode parameter, A-28
hybrid mode, configuring, 3-20

I

inactivity timer
  setting, 3-57
Inactivity Timer Mode parameter, A-44
Inactivity Timer parameter, A-44
inactivity timers, 2-34
inactivity values, setting for SVCs, 3-55
incoming call proceeding state, 2-12
interface parameters, A-1
interface, oversubscribing with traffic shaping, 2-32
IP adjacent hosts, 1-9
IPX adjacent hosts, 1-9

K

K, Max Window Size parameter, A-16

L

LAP-F
  release complete message processing, 2-14
  release message processing, 2-14
LAPF
  active state, 2-9
  call present state, 2-12
  call proceeding processing, 2-13
  call setup processing, 2-12
  categories of management frames, 2-9
  connect message processing, 2-13
  description of, 2-8
  disconnect indication state, 2-12
  disconnect message processing, 2-13
  exchange identification (XID) frames, 2-9
  incoming call proceeding state, 2-12
  N200 retransmission timeout, 2-10
  numbered supervisory frames, 2-9
  operational states, 2-9
  release request state, 2-12
  retransmission timeouts, 2-10
  retransmission timer, 2-10
  setup processing, 2-13
  SVC signaling, 2-8, 2-11
  T200 retransmission timeout, 2-10
  T203 retransmission timeout, 2-11
  TEI-assigned state, 2-9
  timeout timer, 2-9, 2-10
  timer, 2-12
  timer recovery state, 2-9
  unnumbered control frames, 2-9
LAPF parameters
  editing, 3-44
LAPF retransmission timer, 2-9
link management
  call present state, 2-12
  call proceeding processing, 2-13
  call setup processing, 2-12, 2-13
  categories of LAPF management frames, 2-9
  connect message processing, 2-13
  disconnect indication state, 2-12
  disconnect message, 2-13
  exchange identification (XID) frames, 2-9
  incoming call proceeding state, 2-12
  LAPF operational states, 2-9
  LAPF timeout and retransmission timers, 2-9, 2-10
  numbered information frames, 2-9
  numbered supervisor frames, 2-9
  release complete message, 2-14
  release message, 2-14
  release request state, 2-12
  SVC signaling, 2-8, 2-11
  timer
    T303, 2-12
    T305, 2-12
    T308, 2-12
    T310, 2-12
    T322, 2-12
  unnumbered control frames, 2-9
LL Core In Committed Burst parameter, A-50
LL Core In Excess Burst parameter, A-51
LL Core In Throughput parameter, A-48
LL Core Min In Throughput parameter, A-49
LL Core Min Out Throughput parameter, A-48
LL Core Out Committed Burst parameter, A-49
LL Core Out Excess Burst parameter, A-50
LL Core Out Throughput parameter, A-48
LMI (Local Management Interface), 2-7, 3-2, A-5

M

management protocols. *See* DLCMI
management type, selecting, 3-2
Max SVCs parameter, A-18
Mgmnt Type parameter, A-5
monitored events, 3-7
Monitored Events parameter, A-8
moving PVCs, 2-15, 3-17
Multicast parameter, A-9, A-27
multicast, enabling, 3-18
multiline
  configuring, 3-34
  description of, 2-35
  removing, 3-35
  traffic distribution over lines, 2-36
Multiline Algorithm to Choose Line parameter, A-32, A-34

N

N200 retransmission timeout, 2-10
N200, Max Retries parameter, A-16
N201, Max Frame Size parameter, A-16
N322, Status Enq Retry Max parameter, A-21
network congestion, 2-22
numbered information frames, 2-9
numbered supervisory frames, 2-9

O

Options Name parameter, A-41
oversubscribing the interface with traffic shaping, 2-32
overview of frame relay, 2-2

P

packet structure (of frame relay packet), 2-5
pass through, 2-37
polling interval, 3-7
Polling Interval parameter, A-7
present state, 2-12
protocol prioritization
  and multiline, 2-37
  definition of, 2-21
  with traffic shaping, 2-25
protocol priority
  and inactivity timer interaction, 2-35
PVC pass through, 2-37
  configuring, 3-20
PVCs
  adding, 3-14
  configuring on a default service record, 1-6
  definition of, 2-2
  deleting, 3-16
  moving, 3-17
PVCsdefinition of, 2-3

Q

QoS (Quality of Service), 2-25
quality of service, refining for SVCs, 2-28

R

random traffic distribution for multiline, 2-36
release request state, 2-12
Remote Party Number parameter, A-41
Remote Party Number Plan parameter, A-42
Remote Party Sub-Address parameter, A-41
Remote Party Type of Number parameter, A-42
retransmission timeouts, 2-10, 2-11
RFC 1490, 2-18
RIP, and SVCs, 2-35

S

Service Name parameter, A-24, A-36
service record parameters, A-22
service records
  adding, 3-12, 3-35
  default service record, 2-14
  deleting, 3-38
  multiple on an interface, 2-15

Services Multiline With window, A-32
signaling
call proceeding processing, 2-13
call setup processing, 2-12, 2-13
connect message processing, 2-13
SVC, 2-11
signaling parameters
editing, 3-50
Signalling Control parameter, A-18
Site, A-1
source routing using RFC 1490, 2-18
starting frame relay, 1-1
Station Type parameter, A-13
SVC Call Block parameter, A-38
SVC Control parameter, A-43
SVC Inactivity Mode parameter, A-39
SVC Inactivity Timer parameter, A-39
SVC Inscreening Disable parameter, A-38
SVC Inscreening Usage parameter, A-38
SVC Local Party Number parameter, A-36
SVC Local Party Number Plan parameter, A-37
SVC Local Party Sub-Address parameter, A-37
SVC Local Party Type of Number parameter, A-37
SVC Support parameter, A-36
SVCs, 2-12
call proceeding message, 2-13
call proceeding processing, 2-13
call setup processing, 2-12, 2-13
categories of management frames, 2-9
committed information rate (CIR), 2-4
configuring on a default service record, 1-7
connect message, 2-13
connect message processing, 2-13
definition of, 2-2, 2-3
disconnect indication state, 2-12
disconnect message, 2-13
disconnect message processing, 2-13
exchange identification (XID) frames, 2-9
frame relay signaling, 2-8
incoming call proceeding state, 2-12
LAPF and signaling, 2-8
LAPF operational states, 2-9
LAPF timeout and retransmission timers, 2-10
N200 retransmission timeout, 2-10
numbered information frames, 2-9
numbered supervisory frames, 2-9
release complete message, 2-14
release complete message processing, 2-14
release message, 2-14
release message processing, 2-14
release request state, 2-12
retransmission timeout, 2-10
retransmission timeouts, 2-10, 2-11
setup message, 2-12, 2-13
signaling, 2-11
T200 retransmission timeout, 2-10
timers, 2-12
unnumbered control frames, 2-9
SVCs, adding, 3-41
SVCs, disabling, 3-43
synchronous line configuration, 2-39

T

T200 retransmission timeout, 2-10
T200, Base Timer parameter, A-15
T203, Idle Timer parameter, A-15
T303, Setup Message Timer parameter, A-19
T305, Disconnect Timer parameter, A-19
T308, Release Timer parameter, A-20
T310, Call Proceding Timer parameter, A-20
T322, Status Enq Retry Timer parameter, A-21
Technical Solutions Centers, xix
Technician Interface, configuring buffers for traffic shaping, 2-32
TEI-assigned state, 2-9
Throughput parameter, A-29
timer recovery state, 2-9
timers, 2-12
LAPF timeout and retransmission, 2-9, 2-10
N200 retransmission, 2-10
retransmission, 2-10, 2-11
T200 retransmission, 2-10
timeout, 2-10
traffic distribution for multiline, 2-36
traffic shaping, 3-65

buffers, 2-32
configuring committed burst, 2-30
definition of, 2-23
for SVCs, 2-27
guidelines, 2-29
monitoring statistics, 2-30
oversubscribing the interface, 2-32
with data compression, 2-30
Traffic Shaping Disable parameter, A-53

U

unnumbered control frames, 2-9

V

virtual circuits for connections, 2-2

W

WCP Enable parameter, A-54
wfFrCircuitShapedQueueLimit attribute, 2-33
wfFrDlcmiShapingQueueLimit attribute, 2-32
windows
FR PVC List for Service, A-26
Frame Relay Interface List (for PVCs), A-2
Frame Relay PVC Add, A-24
Frame Relay Service List, A-23
Frame Relay Signaling Parameters, A-17
Frame Relay SVC Options Add, A-40
Services Multiline With, A-32

X

X.213 Data LQA Priority parameter, A-45
X.213 Data Priority parameter, A-45
X.213 Gain LQA Priority parameter, A-46
X.213 Gain Priority parameter, A-46
X.213 Keep LQA Priority parameter, A-47
X.213 Keep Priority parameter, A-47
X.213 priority, 2-34
X.213 priority parameters, configuring, 3-71
XOFF bit, setting, 3-11